LAB KEAMANAN KOMPUTER JARINGAN

Disusun Oleh :

Leki Pedri Zela (183510606)

TEKNIK INFORMATIKA

UNIVERSITAS ISLAM RIAU

2020/2021

1. Apa kegunaan shadow password pada linux ?
   Shadow password pada linux kegunaannya adalah menampilkan password yang terenkripsi.
   tetapi tidak menampilkan isi password itu sesungguhnya.

2. Tampilkan password shadow pada system operasi anda ?
   - root@bt:#cat /etc/passwd

```
lekipedrizela@kali:~$ sudo su
[sudo] password for lekipedrizela:
root@kali:/home/lekipedrizela# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:103:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/var/run/iodine:/usr/sbin/nologin
miredo:x:112:65534::/var/run/miredo:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:114:119::/nonexistent:/usr/sbin/nologin
rtkit:x:115:120:RealtimeKit,,,:/proc:/usr/sbin/nologin
_rpc:x:116:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:117:122::/var/lib/snmp:/bin/false
statd:x:118:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:x:119:124:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
stunnel4:x:120:126::/var/run/stunnel4:/usr/sbin/nologin
sshd:x:121:65534::/var/sshd:/usr/sbin/nologin
sslh:x:122:127::/nonexistent:/usr/sbin/nologin
avahi:x:123:128:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
nm-openvpn:x:124:129:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:125:130:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbi
n/nologin
pulse:x:126:132:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
saned:x:127:134::/var/lib/saned:/usr/sbin/nologin
inetsim:x:128:136::/var/lib/inetsim:/usr/sbin/nologin
colord:x:129:137:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:130:138::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
```

```
geoclue:x:130:138::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:131:139:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nologin
lekipedrizela:x:1000:1000:LekiPedriZela,,,:/home/lekipedrizela:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
leki:x:1001:1001::/home/leki:/bin/sh
lekipedri:x:1002:1002::/home/lekipedri:/bin/sh
root@kali:/home/lekipedrizela#
```

- root@bt:#cat /etc/shadow

```
root@kali:/home/lekipedrizela# cat /etc/shadow
root:!:18564:0:99999:7:::
daemon:*:18564:0:99999:7:::
bin:*:18564:0:99999:7:::
sys:*:18564:0:99999:7:::
sync:*:18564:0:99999:7:::
games:*:18564:0:99999:7:::
man:*:18564:0:99999:7:::
lp:*:18564:0:99999:7:::
mail:*:18564:0:99999:7:::
news:*:18564:0:99999:7:::
uucp:*:18564:0:99999:7:::
proxy:*:18564:0:99999:7:::
www-data:*:18564:0:99999:7:::
backup:*:18564:0:99999:7:::
list:*:18564:0:99999:7:::
irc:*:18564:0:99999:7:::
gnats:*:18564:0:99999:7:::
nobody:*:18564:0:99999:7:::
_apt:*:18564:0:99999:7:::
systemd-network:*:18564:0:99999:7:::
systemd-resolve:*:18564:0:99999:7:::
systemd-timesync:*:18564:0:99999:7:::
mysql:!:18564:0:99999:7:::
tss:*:18564:0:99999:7:::
strongswan:*:18564:0:99999:7:::
ntp:*:18564:0:99999:7:::
messagebus:*:18564:0:99999:7:::
redsocks:!:18564:0:99999:7:::
rwhod:*:18564:0:99999:7:::
iodine:*:18564:0:99999:7:::
miredo:*:18564:0:99999:7:::
usbmux:*:18564:0:99999:7:::
tcpdump:*:18564:0:99999:7:::
rtkit:*:18564:0:99999:7:::
_rpc:*:18564:0:99999:7:::
Debian-snmp:!:18564:0:99999:7:::
statd:*:18564:0:99999:7:::
postgres:*:18564:0:99999:7:::
stunnel4:!:18564:0:99999:7:::
sshd:*:18564:0:99999:7:::
sslh:!:18564:0:99999:7:::
avahi:*:18564:0:99999:7:::
nm-openvpn:*:18564:0:99999:7:::
nm-openconnect:*:18564:0:99999:7:::
pulse:*:18564:0:99999:7:::
saned:*:18564:0:99999:7:::
inetsim:*:18564:0:99999:7:::
colord:*:18564:0:99999:7:::
geoclue:*:18564:0:99999:7:::
lightdm:*:18564:0:99999:7:::
king-phisher:*:18564:0:99999:7:::
lekipedrizela:$6$1iBoT9zSwkUtD1AG$Mdk2sw2FSAPyW/2FRREYxCdo/CiZuaX28faxi6jSs5ECivw1KsqVDG6XQupG8q1sCXc5.Kyc0qIvmyjJM8T2g1:18564:0:99999:7:::
systemd-coredump:!*:18564::::::
```

```
lightdm:*:18564:0:99999:7:::
king-phisher:*:18564:0:99999:7:::
lekipedrizela:$6$1iBoT9zSwkUtD1AG$Mdk2sw2FSAPyW/2FRREYxCdo/CiZuaX28faxi6jSs5ECivw1KsqVDG6XQupG8q1sCXc5.Kyc0qIvmyjJM8T2g1:18564:0:99999:7:::
systemd-coredump:!*:18564::::::
leki:$6$UjodQhSUZVDPWx5O$yF3Itk0iJ5EVECbXokVQdwcKT4axROW6ynbnpIkSlV01A7fKLXksff1xW1obDLqlwUF437sh9nkKRt5GheGZO1:18629:0:99999:7:::
lekipedri:$6$x0FUsV9tjxM9rDtF$qMwZTqw9YlHMCIrtvRDXvoEPpjWBvmEw/wPKcmz7AKw.kbjgPBWraCJCL.i/IwIqoXopEaR.a2g.PJXk9lffd1:18629:0:99999:7:::
root@kali:/home/lekipedrizela#
```

3. Buatlah user baru, lalu implementasikan crack pada user tersebut
   - Membuat user baru

```
root@kali:/home/lekipedrizela# useradd Lekipedrizelaa
root@kali:/home/lekipedrizela# passwd lekipedrizelaa
passwd: user 'lekipedrizelaa' does not exist
root@kali:/home/lekipedrizela# useradd Lekipedrizelaa
useradd: user 'Lekipedrizelaa' already exists
root@kali:/home/lekipedrizela# passwd lekipedrizelaa
passwd: user 'lekipedrizelaa' does not exist
root@kali:/home/lekipedrizela# passwd Lekipedrizelaa
New password:
Retype new password:
passwd: kata sandi diperbaharui dengan sukses
root@kali:/home/lekipedrizela#
```

```
passwd: kata sandi diperbaharui dengan sukses
root@kali:/home/lekipedrizela# unshadow /etc/passwd /etc/shadow > unshadowed.txt
root@kali:/home/lekipedrizela#
```

```
root@kali:/home/lekipedrizela# john unshadowed.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 3 password hashes with 3 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Further messages of this type will be suppressed.
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
```

- Melihat password menggunakan john

```
root@kali:/home/lekipedrizela# john --show unshadowed.txt
lekipedrizela:123456:1000:1000:LekiPedriZela,,,:/home/lekipedrizela:/bin/bash

1 password hash cracked, 3 left
```