

**TUGAS KEAMANAN JARINGAN KOMPUTER
CRACK PASSWORD LOGIN PADA KALI LINUX**



NAMA : Sri Retno Rahayu

NIM: 09011381621069

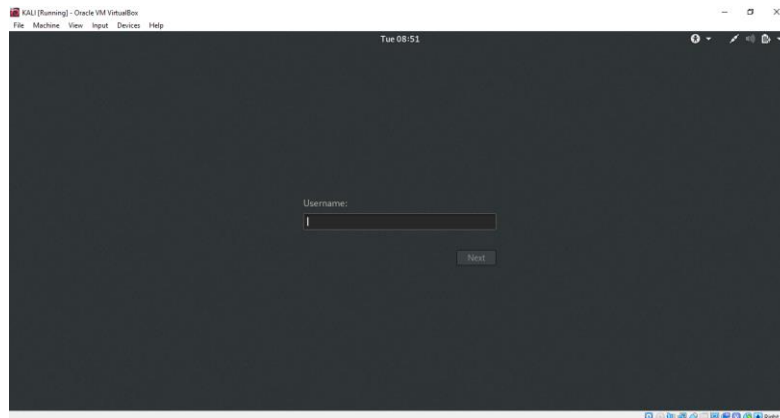
**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

2019

Pada tugas cracking password kali ini saya menggunakan tools **John The Ripper** di sistem operasi Kali Linux.

Langkah-Langkah :

1. Lakukan instalasi OS Kali Linux di VirtualBox, setelah instalasi masukkan username root dan password nya.



2. Setelah login, cek apakah tools John The Ripper sudah terinstall atau belum dengan cara mengetik john pada terminal

```
root@osboxes:~# john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,...]] "single crack" mode, using default or named rules
--single=rule[,...] same, using "immediate" rule(s)
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
--pipe like --stdin, but bulk reads, and allows rules
--loopback[=FILE] like --wordlist, but extract words from a .pot file
--dupe-suppression suppress all dupes in wordlist (and force preload)
--prince[=FILE] PRINCE mode, read words from FILE
--encoding=NAME input encoding (eg. UTF-8, ISO-8859-1). See also
doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,...]] enable word mangling rules (for wordlist or PRINCE
--rules=:rule[;,...] modes), using default or named rules
--rules-stack=SECTION[,...] same, using "immediate" rule(s)
--rules-stack=:rule[;,...] stacked rules or to
--rules-stack=:rule[;,...] modes that otherwise don't support rules
--incremental[=MODE] same, using "immediate" rule(s)
--mask[=MASK] "incremental" mode [using section MODE]
--markov[=OPTIONS] mask mode using MASK (or default from john.conf)
--external=MODE "Markov" mode (see doc/MARKOV)
--subsets[=CHARSET] external mode or word filter
--stdout[=LENGTH] "subsets" mode (see doc/SUBSETS)
--restore[=NAME] just output candidate passwords [cut at LENGTH]
--session=NAME restore an interrupted session [called NAME]
--status[=NAME] give a new session the NAME
--make-charset=FILE print status of a session [called NAME]
--show[=left] make a charset file. It will be overwritten
show cracked passwords [if =left, then uncracked]
```

Jika tampilannya sudah seperti itu berarti tools John The Ripper sudah terinstall.

3. Jika kita ingin melihat apa password yang digunakan oleh user root dan user lainnya kita harus crack passwordnya. Cara yang menurut saya sedikit lebih mudah adalah dengan menggunakan file shadow yang ada dalam tools John The Ripper , karena

setiap password linux tersimpan kedalam file. Buka terminal dan klik : john /etc/shadow

```
root@osboxes:~# john /etc/shadow
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)
root@osboxes:~#
```

Jika tampilan yang muncul seperti ini artinya sudah ada 2 password yang berhasil di crack . Untuk menampilkannya tambahkan perintah --show : john --show /etc/shadow . Maka akan muncul password yang sudah di crack sebelumnya beserta usernamenya.

```
root@osboxes:~# john --show /etc/shadow
root:12345:18233:0:99999:7:::
srr:password:18233:0:99999:7:::

2 password hashes cracked, 0 left
root@osboxes:~#
```

Dengan demikian crack password pada kali linux telah berhasil dilakukan.