CMPUT 333

SECURITY IN A NETWORKED WORLD

Lab Assignment 1:
John the Ripper

Block cipher modes of operation

Part 3

- **Encryption command:**
  “openssl enc -e -des-XYZ -nosalt -in plaintext -out cipherXYZ.enc”
- **You can use the ‘xxd’ command, when you need to replace the 19th byte with a different byte**
- **Make sure to explain the reasons for your observations**
- **For information about the different block cipher modes you can check Wikipedia:**

  https://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

PASSWORD CRACKING

John the Ripper

Steps

1. **Download John the Ripper**
   - http://www.openwall.com/john/j/john-1.8.0-jumbo-1.tar.gz
   - Note you want the JUMBO version of John the Ripper. This supports the -format=nt flag which you will likely need.
   - **Extract the file on your Desktop**
   - tar –xzf john-1.8.0-jumbo-1.tar.gz

3. **Compile the source file as follows:**
   - Navigate to the extracted folder ‘john-1.8.0-jumbo-1’
   - Navigate to src/
   - Enter the command “./configure && make ”

4. **A ‘john’ executable will be created in the** ‘../john-1.8.0-jumbo-1/run’ directory

5. **You can test that it works** by navigating in the directory mentioned in step 4 through your console and by entering: ./john --test

PASSWORD CRACKING

Documentation

- doc/README – general information
- doc/EXAMPLES – usage examples
- doc/MODES – the different cracking modes
- doc/RULES – wordlist mangling rules

Read the documentation of the different modes in order to decide which ones can help you the most. And look in doc/EXAMPLES to see how modes are used.

PASSWORD CRACKING

John the Ripper

Wordlist mode

- Given a list of words, will try each of them
- Mangling rules: allows applying various transformations to the words in the list
  - Specified in 'john.conf' in the run folder
  - Documentation in doc/RULES
  - You can also produce customized wordlist using your own code
- doc/MODES for more details

PASSWORD CRACKING

John the Ripper

Single crack mode

- Will use information in the password list
  - Usernames, real names, etc.
- Will apply a variety of mangling rules
  - Specified in 'john.conf'
  - Documentation in doc/RULES
- See doc/MODES for more details

PASSWORD CRACKING

John the Ripper

Incremental mode

- Brute force mode
- Can be used if nothing else works
- Can specify min/max length and character set in john.conf
- doc/MODES for more details

Machine-Use Etiquette & Tips

- When running John the Ripper (or any other time consuming lengthy process) you need to ***nice*** your process
  - *nice* is a command that sets the **priority** of your job from -20 (very high priority) to 19 (very low priority)
  - your commands typically have a default priority of 0
  - **you must run your password cracking programs with a nicenesss level of 19**
  - *http://www.thegeekstuff.com/2013/08/nice-renice-command-examples/*
  - ps -l lets you see the niceness of your processes (under the Ni column)

Machine-Use Etiquette & Tips

- While machine-usage etiquette is to **never reboot a lab machine** without lab admin permission, sometimes reboots happen.
- **An interrupted session can be restored** by starting john the ripper using the —restore flag.
- More details in docs.

You **MUST ONLY** use your group lab machine.

If you see suspiciously large processes running for long periods of time, contact the TAs and we will investigate.

Extra Reminders

Make sure you describe everything you do in the assignment report.

Be clear on any assumptions you had and explain your motivation for any choices you made.

Make sure to check the forum for hints.

Post questions to the forums and feel free to share anything interesting or useful you come across! The forums are as helpful as you make them :)

QUESTIONS?