John the Ripper step-by-step tutorials for end-users

Tutorials maintained on this wiki:

- How to build on Ubuntu Linux (basic to intermediate)
- How to build on/for Win64 (basic to intermediate)
- Cracking/auditing user passwords on recent Ubuntu, Fedora, and some Solaris 10+ (SHA-crypt) (basic to intermediate)
- How to retrieve and audit password hashes from remote Linux servers (intermediate)
- Cracking WPA-PSK/WPA2-PSK with John the Ripper (intermediate)
- Procedure to add a new code-page to john (advanced development - should move out of tutorials!)
- OpenCL BitLocker tutorial

External links (English):

- Comprehensive Guide to John the Ripper (in 7 parts so far) [https://miloserdov.org/?p=4961] (basic to advanced)
- Password cracking with John the Ripper on Linux [https://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux] using distro-provided packages (basic)
- Cracking Tezos ICO passwords on Windows 10 [https://medium.com/@miningroi/cracking-tezos-ico-passwords-on-windows-10-43d8462adaec] (basic to intermediate; detailed step by step with pictures)
- Cracking Tezos ICO passwords on macOS, OSX, Apple [https://medium.com/@miningroi/cracking-tezos-ico-passwords-on-osx-6802253df1b9] (basic to intermediate; detailed step by step with pictures)
- JtR Active Directory Password Auditing / NTDS.dit extraction (by Rich Rumble) [https://xinn.org/blog/JtR-AD-Password-Auditing.html] (basic to intermediate)
- Password Cracking Class for Hackers For Charity - video of 3 talks on password cracking history and modern techniques [http://www.irongeek.com/i.php?page=videos/password-cracking-class-hfc-louisville-issa] (download links [https://archive.org/details/ISSAKentuckianaPasswordCrackingClass]), a JtR usage tutorial is talk 2 starting at ~7000 seconds or ~1:56:40 (basic to intermediate)
- There are many video tutorials/demos for specific uses of JtR on YouTube [http://www.youtube.com/results?search_query=%22john+the+ripper%22] (mostly basic stuff)
- How to quickly crack NTLM hashes given cracked LM hashes [http://www.room362.com/blog/2012/10/24/lm2ntlm-with-john-the-ripper.html] (intermediate)
- Building and using John the Ripper with OpenMP support (to use multiple CPU cores) [http://blog.thireus.com/crack-passwords-using-john-the-ripper-with-multiple-cpu-cores-openmp] (basic)
- Step-by-Step Clustering JtR with MPI on Kali Linux (by Luis Rocha) [http://countuponsecurity.com/2015/05/07/step-by-step-clustering-john-the-ripper-on-kali/] (basic)
- JtR Cheat Sheet (by Luis Rocha) [https://countuponsecurity.com/2015/06/14/jonh-the-ripper-cheat-sheet/] (basic)
- Building and using John the Ripper with MPI support (to use multiple CPU cores, maybe across multiple machines), also adding a custom hash type based on MD5 and SHA-1 [http://blog.thireus.com/john-the-ripped-steak-and-french-fries-with-salt-and-pepper-sauce-for-hungry-password-crackers] (intermediate to advanced)
- A generic tutorial rehashing much of the official documentation [http://juggernaut.wikidot.com/jtr] (mostly basic). This one has numerous factual errors, yet it is representative of what many JtR tutorials look like, and all of them contain factual errors, unfortunately (please feel free to submit a better one or to write one right on this wiki).
- Downloading and building JtR with the jumbo patch on Linux [http://www.jedge.com/wordpress/?p=233] (intermediate)
- Running the official build of JtR 1.7.0.1 under Windows to crack sample passwords [http://www.profsam.com/406/jtr.html] (basic)
- Cracking Mac OS X salted SHA-1 passwords (by Patrick Dunstan) [http://www.defenceindepth.net/2009/12/cracking-os-x-passwords.html] (intermediate, comments)

- Making an advanced build of JtR with patches on Mac OS X Snow Leopard (by Matt Weir) [http://sites.google.com/site/reusablesec/Home/john-the-ripper-files/tutorials] (comments [http://www.openwall.com/lists/john-users/2009/11/18/1])
- How-to: John the Ripper on a Ubuntu 10.04 MPI Cluster (by Pétur Ingi) [http://www.petur.eu/blog/?p=59], also available as a PDF file [http://www.petur.eu/projects/John_the_Ripper_on_a_Ubuntu_10.04_MPI_Cluster.pdf] (intermediate)
- Parallelizing JtR across multiple CPU cores using MPI on a Red Hat'ish Linux system (by Hamid Kashfi) [http://hkashfi.blogspot.com/2008/12/how-to-make-johntr-use-all-of-your-cpu.html] (intermediate)
- Using Wireshark and John to crack LEAP [http://intellavis.com/blog/?p=138] (advanced, skips the patching step)
- Dumping the user's password hash on Mac OS X 10.5 via the ARDAgent vulnerability, cracking the hash [http://www.hackint0sh.org/f154/44968.htm] (intermediate). The specific download URL for a JtR build is outdated, use a more recent version/build [http://www.openwall.com/john/#contrib] instead.
- Automatically generating wordlist mangling rules [http://en.wordpress.com/tag/mangling-rules-generation/] (advanced)
- Why we need strong p4ssw0rds: a blog post about password cracking and John the Ripper [http://codebazaar.blogspot.com/2011/05/why-we-need-strong-p4ssw0rds.html] (basic to intermediate; an example unnecessarily uses the "external mode" where a simpler wordlist rule would do)
- Supercharged John the Ripper Techniques [https://www.owasp.org/images/a/af/2011-Supercharged-Slides-Redman-OWASP-Feb.pdf] by Rick Redman of KoreLogic (PDF file with slides; basic to intermediate)
- Downloading and cracking RACF hashes [http://mainframed767.tumblr.com/post/43072129477/how-to-copy-the-racf-database-off-the-mainframe-and] (basic)

External links (non-English):

- Portuguese tutorial on compiling and using JtR 1.7 under Linux [http://www.vivaolinux.com.br/artigo/Auditando-senhas-com-John-The-Ripper] (basic, split over 8 web pages)
- Spanish blog posts on using JtR under Ubuntu - parts 1 [http://sliceoflinux.com/2009/03/26/john-the-ripper-i-comprueba-la-fortaleza-de-tu-contrasena-en-ubuntu/], 2 [http://sliceoflinux.com/2009/07/03/john-the-ripper-ii-comprueba-la-fortaleza-de-tu-contrasena-en-windows/], 3 [http://sliceoflinux.com/2010/03/26/john-the-ripper-iii-comprueba-la-fortaleza-de-tu-contrasena-en-ubuntu-9-10/] (basic to intermediate)
- Icelandic version of Pétur Ingi's JtR/Ubuntu/MPI how-to, PDF file [http://www.petur.eu/projects/John_the_Ripper_on_a_Ubuntu_10.04_MPI_Cluster_ICELANDIC.pdf] (intermediate)
- Russian version of the JtR/Ubuntu/MPI how-to, web page with reader comments [http://www.opennet.ru/tips/2542_mpi_cluster_johntheripper_mpich_ubuntu_hash.shtml] (intermediate)

What content to add

I think that this wiki page/section should contain primarily simple stuff aimed at typical end-users. I envision these tutorials as step-by-step guides or examples for specific use cases - e.g., auditing passwords on a Windows system (that's one tutorial), then auditing passwords from various Unix-like systems and Windows on a Linux system (that's another tutorial). And I do mean step-by-step - e.g., start with downloading JtR, compiling it (if applicable), downloading pwdump6 [http://www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista#pwdump] and running it on a Windows system with output to a file, scp'ing the file, and so on… More specific and with greater detail than that found in the official documentation [http://www.openwall.com/john/doc/] for JtR. Some overlap with the official documentation (such as with doc/EXAMPLES [http://www.openwall.com/john/doc/EXAMPLES.shtml]) and between multiple tutorials is no problem. Right now, this page mostly links to external websites, which is OK, but I would actually prefer that

tutorials be written right on this wiki, with new pages created under this “tutorials” DokuWiki namespace. - solar

Back to John the Ripper user community resources.