

TRACK: IT Security
SESSION #: IT#9
DATE: Tuesday April 20, 2010
TIME: 2:55-4:10pm
SESSION TITLE: "Cracking 2.1 Million Passwords - Supercharged John the Ripper Techniques"
SPEAKER(S): Rick Redman – Senior Security Consultant
ORGANIZATION: KoreLogic, Inc.

ABSTRACT: "Cracking 2.1 Million Passwords - Supercharged John the Ripper Techniques"

Password crackers such as John the Ripper ("JtR") are an integral part of a forensic practitioner's toolkit. However, many of us just use the default "rules" defined in the configuration file rather than using optimized rules. In this presentation, we will demonstrate the types of passwords JtR can crack using the default rule-set (using real world examples). Then, we will demonstrate (using a PWDUMP output file containing 49,000+ real "complex" NTLM passwords) how JtR's default rule-set can be improved to crack tens of thousands of additional passwords. The presentation will include numerous real world examples, and attendees will leave with a large bag of tricks that will be immediately beneficial to your password cracking efforts. This class is not a tutorial on how to use JtR - but instead how to fully leverage its power by training you to read and write new optimized JtR rules.

What will attendees gain from the presentation?

All attendees will leave the presentation with a set of new rules, word-lists, and tricks/tips that will drastically improve their ability to crack passwords. In addition, attendees with less experience will gain insight into how passwords are obtained, and how their passwords can be easily cracked by analyzing human nature's desire to create passwords that can be remembered (but still meet with password policy requirements).

Presentation outline

- 1) A short introduction to John the Ripper / What it does / How to use it.
- 2) Demonstrate what types of passwords John the Ripper can crack using the default rule-set (using real world examples) - Provide statistics on how many of these passwords were cracked using the default rule-set. Establishes our "baseline" for what is possible with John the Ripper using the default rule-set.
- 3) Illustrate the delta between default rule-set performance and using optimized rules. This will be done by demonstrating a list of 20000+ passwords that were cracked using more customized procedures/rules. The goal of this section is to allow the audience to look at the passwords and think "Hey, I see some really easily recognizable patterns in that list! Why didn't those passwords crack? How can I make John the Ripper crack passwords like that?"
- 4) Review the patterns found in the list of 20000+ cracked passwords, and create new John the Ripper rules (or word-lists). We will begin with a few basic examples (i.e. use most obvious patterns) then move to more complex examples.
- 5) Next, we will present other 'tricks' that can be used to crack even more passwords using built in (but rarely used) functionality provided by John the Ripper. Wordlists will be shared (along with how to create them), shell scripts that help split large amounts of work into smaller bits, methods for manipulating previously cracked passwords into new possibilities, etc.

SPEAKER BIO(S): During his 11 years as a security practitioner, Rick has delivered numerous application and network penetration tests for a wide range of Fortune 500 and government clients. Rick serves as KoreLogic's subject matter expert in advanced password cracking systems. Rick presents at a

variety of security forums such as ISSA Chapters and AHA (Austin Hackers Anonymous) and provides technical security training on topics such as web application security. Rick has served as a member of a penetration testing tiger team supporting Sandia National Laboratories. Mr. Redman is a graduate of Purdue University with a degree in Computer Science in the CERIAS/COAST program taught by Gene Spafford.