What You Can Learn from Bad Guys and Hackers About Cracking Passwords

Rick Redman
Senior Security Consultant, KoreLogic

Governance, Risk & Compliance – G24

Session Abstract

In the last 2-3 years, a new trend has popped up in the "hacker" community. Attackers are no longer JUST defacing web-sites, they are publishing entire database dumps of any website that has been compromised. In June 2012, it was made public (finally!) that database dumps of LinkedIn, eHarmony, Last.fm were all available on the Internet.

Anyone could download these dumps, and extract the password hashes, and crack millions and millions of passwords. Not only are the database leaks available, put people are sharing their CRACKED passwords as well.

What can we learn from all this? How can we better protect our systems from this type of release of information? How can we protect our users if they have accounts on these web-sites? How can we audit our own password hashes? How can we improve our password cracking techniques?

In this talk Rick Redman will talk about the password leaks, show how they were released, how they were cracked, and how you can become a password cracker as well. Rick will also expose you to the password cracking community and show you the statistics that prove just how bad our users are at choosing passwords.

Target Audience

Anyone who has ever used a password to protect anything needs to be at this talk. System administrators, managers of users, auditors and testers.

COBIT Objectives

N/A

Speaker Bio

Rick Redman has been testing web application security and a penetration tester since 1999. He founded and runs the DEFCON password cracking contest "Crack Me If You Can." He started out by running a BBS in the early 1993 and selling UUCP based Internet from a 486dx33. After graduating from Purdue's COAST/CERIAS program in the 90s under 'spaf' he hit the ground running being a penetration tester by working on projects such as Sandia National Lab's "Tiger Team." Rick made the rounds in 2010-2012 giving talks about advanced password cracking, including being on the closing panel at ShmooCON.

Rick works for KoreLogic as a Senior Security Consultant doing "by hand" penetration tests for large corporate environments. Rick was also one of the first security researchers to identify the "LinkedIn" password leaks a day before the news hit the Internet.