MySQL Passwords

Password Strength and “Cracking”

Presented by Devin Egan

Defcon 12 - July 31, 2004

Introduction

- Who am I?
- Goals
  - MySQL Password Education
  - Introduce MySQL Password “Cracking”

What Will This Talk Cover?

- Covered

  MySQL Password “Cracking”

- NOT covered

  How to obtain a MySQL hash

Passwords: Best Practices

- Absolute Minimum of 9 Characters
- Mixed Case and Mixed Special Characters

Why Crack MySQL Passwords?

- Security Audits
- Recovery of a lost password

Tools for Cracking Passwords

- Existing tools

  "mysqlfast"

  - Very effective and fast Brute Force Cracker
  - Limited:

    8 characters max

    Works only on a hash for MySQL 4.0 or lower

    Single hash at a time

Tools for Cracking Passwords

- Existing tools

  "John The Ripper" (contrib)

  - Dictionary-based Cracker
  - Trusted by most security professionals
  - Limited:

    Works only on a hash for MySQL 4.0 or lower

    Can be SLOW

Tools for Cracking Passwords

- New Tool

  "phpMyAudit"

  - Dictionary-based
  - Runs from the Web or a Shell Script
  - Extremely fast (after dictionary import)
  - Can find passwords that "mysqlfast" cannot brute force
  - Limited:

    Not always as effective as "mysqlfast" or "John"

Demonstration!

Conclusion

- Questions?

For updates, please check:

http://www.php5security.com/projects/phpMyAudit