Password cracking in the field

operating systems and database management systems

Research Project 1

Gert Bon
Steffen van Loon

Inhoud

- Introductie opdrachtgever
- Keuze projectvoorstel
- Onderzoeksdoelen
- Aanpak
- Resultaat
- Verschillende conclusies
- Aanbevelingen
- Toekomstige ontwikkelingen
- “Watch yourself!”

Introductie KPMG IRM

- 3000 medewerkers in NL

- Information Risk Management
- Ruim 200 medewerkers

Keuze projectvoorstel

- Meerdere opties
- Verdieping n.a.v. SSN
- Security is hot issue

Onderzoeksdoelen

- Een overzicht van encryptie algoritme implementaties in populaire software
- Aanvalstechnieken
- Invloed op implementaties en zwakheden

Aanpak

- 2 mogelijke:
  - Verzamel informatie; daarna report schrijven
  - Verzamel informatie; verwerk gelijk in report
- Conclusie gekozen aanpak
  - Teveel informatie om te verwerken
  - Werkdruk laatste week

Resultaat

- Wel aan toegekomen
  - Karakteristieken voor een aantal implementaties
  - Informatie t.b.v. beveiliging systemen & netwerken
- Niet aan toegekomen
  - Implementaties in o.a. WPA-PSK, HP-UX en LDAP

Verschillende conclusies

- Resultaten
  - Gebruikte techniek is meestal goed
  - Gebruikte implementatie is vaak slecht

  - "*There is no patch for human stupidity*"

Aanbevelingen

- Implementatiespecifiek
- Advies passwords
- Pass phrases
- Advies Rainbow

Toekomstige ontwikkelingen

- Toenemend gevaar rainbow tables
  - Downloadbare rainbow tables
  - Sites met online crack mogelijkheid
  - Cain met Rainbowcrack-Online cliënt
  - Mogelijk gebruik van rainbow tables op andere implementaties

Watch yourself

- Tabellen voor:
  - LM / NTLM / MD2 / MD4 / MD5
  - SHA1 / RIPEMD-160
  - MySQL v3.23 / MySQL SHA1 / Cisco PIX
- MD5:
  - -uit privacy overwegingen verwijdert-

Vragen

- Zijn er nog vragen?