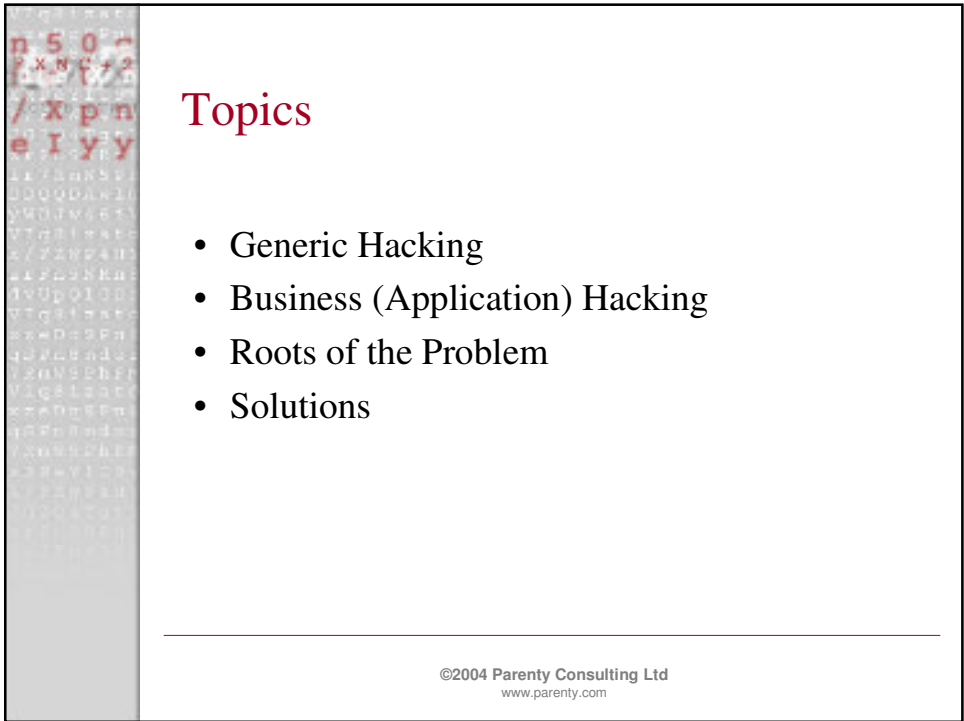


Digital Hacking

Thomas Parenty
Managing Director, Parenty Consulting Limited

Information Systems Audit and Control Association
Hong Kong Chapter Professional Development Seminar
5 August 2004



Topics

- Generic Hacking
- Business (Application) Hacking
- Roots of the Problem
- Solutions

©2004 Parenty Consulting Ltd
www.parenty.com



(Generic) Hacking

- Attack networks, operating systems, and general purpose applications, e.g., web server
- Has nothing to do with what target company does for a living
- Get Root/Administrator privilege and Go
- Useful/Dangerous (depends on perspective)

©2004 Parenty Consulting Ltd
www.parenty.com



Business (Application) Specific

- Understand business processes (applications)
- Target what you want to steal
- Don't need to take over the world
- Focus on bypassing security checks
 - User authentication
 - Access control

©2004 Parenty Consulting Ltd
www.parenty.com



Session IDs: Maintaining State

- URL encoding
- Hidden HTML fields
- Cookies
 - Per-session: in memory
 - Persistent: written to disk

©2004 Parenty Consulting Ltd
www.parenty.com



On-line Corporate Education

- ASP hosts courses for many companies
 - Sales training
 - Proprietary content
- User logs on, requests course, access checked
- Course ID in URL string
 - Predictable: includes company name
 - Change course ID, no additional access check
 - Get new course
- Same tactic for User Session ID

©2004 Parenty Consulting Ltd
www.parenty.com



Shopping Cart Applications

- On-line clothing store
- Shopping cart stored in per-session cookie
 - Including price
- Change price in cookie
- Get “sale price”

- How?

©2004 Parenty Consulting Ltd
www.parenty.com




Achilles

- Web proxy
- Intercepts/Freezes/Edits all traffic
 - Cookies
 - Hidden form elements
 - SSL-encrypted traffic

- <http://www.mavensecurity.com/achilles>

©2004 Parenty Consulting Ltd
www.parenty.com



Reasons for these Vulnerabilities

- Application developers didn't understand:
 - What information needed to be protected
 - What the risks were
 - What security technology was required


©2004 Parenty Consulting Ltd
www.parenty.com



Development Solutions

- Start with business operation
 - Taking an on-line course
 - Buying a pair of pants
- Identify information critical to operation
- What protection and control does it need?
- What are the threats?
- Develop/choose security solution


©2004 Parenty Consulting Ltd
www.parenty.com



Security Mantras

- Why do I believe this (information, process) is protected?
- What else needs protection to ensure security of business operation?

©2004 Parenty Consulting Ltd
www.parenty.com



Questions and Answers

Digital Hacking

Thomas Parenty
Managing Director, Parenty Consulting Limited
tparenty@parenty.com

Event
5 August 2004