

Penetrating the “Unbreakable” Oracle

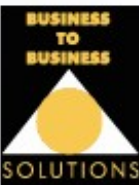
Presented by

Paul Stallard

pstallard@b2bsol.com

Business to Business Solutions, LLC

Web: www.b2bsol.com



Agenda

- Current Database Security Environment
- Common Attack Techniques
- Mitigating Risk



Current Database Security Environment

“Slump Prompts Workplace Snooping”

- Survey of IT works within large British and American companies
- 35% had viewed confidential information (e.g. salaries)
- 74% said they could get around controls designed to secure confidential information
- Many stated they would steal information such as customer data, passwords, company plans etc.



Current Database Security Environment

“Oracle Users Struggle with Patch Management”

- Independent Oracle Users Group (IOUG) study published Feb. '09: nearly half of Oracle users were at least two or more patch cycles behind; 8% four or more cycles behind; 11% had never applied a CPU
- Sentrigo (database security software provider) study this year: only 10% of users had applied latest CPU; more than two-thirds had never applied a CPU.



Current Database Security Environment

Hannaford, 7-Eleven, and Heartland Payment Systems

- Called largest identify theft case ever prosecuted
- Data from more than 130 million debit and credit cards alleged stolen from Heartland alone
- Sql Injection used to gain access to systems



Common Attack Techniques

SQL Injection

- Insufficiently or unvalidated literal strings are concatenated into a dynamic SQL statement and interpreted



Common Attack Techniques

SQL Injection

1. First Order

- malicious string is entered and resulting code is executed immediately
- e.g. “select * from users where password = '|| inputpw||';” ... replace inputpw with “ or 1=1 --”

1. Lateral Injection

- can be used to exploit procedure that does not take user input
- cause the database to accept arbitrary SQL as a date or number

Common Attack Techniques

SQL Injection

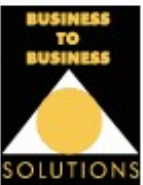
DEMO



Common Attack Techniques

Privilege Escalation

DEMO



Mitigating Risk

- **Vulnerability Assessment**
 - Knowing where you stand with regard to security holes and configuration
- **Hardening**
 - Implementing recommendations from the Vulnerability Assessment
 - Eliminating functions and options that are not used
- **Asset Assessment**
 - What are your sensitive databases and where is your sensitive data



Mitigating Risk

- Asset Assessment (cont.)
 - Data likes to replicate: dev/test databases, user extracts
 - An ongoing process that ideally has is somewhat automated
- Patch Management
 - Testing is important but emphasis should be on why a patch should not be applied versus why it should
 - Can greatly benefit from automation solutions, e.g. Oracle Enterprise Manager database control and grid control



Mitigating Risk

- Database Activity Monitoring
 - Real-time knowledge of who and what is being done in your databases
 - Can alert you to unusual access patterns, attacks, unauthorized access
- Auditing
 - Audit data needs to be secure, reviewed (automated), and produce minimal impact on performance



Mitigating Risk

- Authentication and Access Control
 - Not all data or users are created equal
 - Manage privileges to limit access
- Encryption
 - Highly sensitive data should be encrypted within the database
 - To be effective encryption needs to take place with data in-transit and at rest



Resources

Oracle Security

Pete Finnigan - <http://www.petefinnigan.com>

David Litchfield - <http://www.davidlitchfield.com>

Red Database Security - <http://red-database-security.com>

Sentrigo Software - <http://www.sentrigo.com>

Oracle Forensics - <http://www.oracleforensics.com>

General Penetrating Testing/Exploit Framework

Metasploit Project - <http://www.metasploit.com>