

THE ORACLE HACKER'S HANDBOOK: HACKING AND DEFENDING ORACLE

About the Author.

Acknowledgments.

Introduction.

Code Samples from the Book.

Oracle and Security.

The Unbreakable Marketing Campaign.

Independent Security Assessments.

The Future.

Chapter 1 Overview of the Oracle RDBMS.

Architecture.

Processes.

The File System.

The Network.

Database Objects.

Users and Roles.

Privileges.

Oracle Patching.

Wrapping Up.

Chapter 2 The Oracle Network Architecture.

The TNS Protocol.

The TNS Header.

Inside the Packet.

Getting the Oracle Version.

The Listener Version and Status Command.

Using the TNS Protocol Version.

Using the XML Database Version.

BUY ONLINE AT: <http://www.itgovernance.co.uk/products/1249>

Using TNS Error Text.

Using the TNS Version TTC Function.

Wrapping Up.

Chapter 3 Attacking the TNS Listener and Dispatchers.

Attacking the TNS Listener.

Bypassing 10g Listener Restrictions.

The Aurora GIOP Server.

The XML Database.

Wrapping Up.

Chapter 4 Attacking the Authentication Process.

How Authentication Works.

Attacks Against the Crypto Aspects.

Default Usernames and Passwords.

Looking in Files for Passwords.

Account Enumeration and Brute Force.

Long Username Buffer Overflows.

Wrapping Up.

Chapter 5 Oracle and PL/SQL.

What Is PL/SQL?

PL/SQL Execution Privileges.

Wrapped PL/SQL.

Wrapping and Unwrapping on 10g.

Wrapping and Unwrapping on 9i and Earlier.

Working without the Source.

PL/SQL Injection.

Injection into SELECT Statements to Get More Data.

Injecting Functions.

Injecting into Anonymous PL/SQL Blocks.

BUY ONLINE AT: <http://www.itgovernance.co.uk/products/1249>

The Holy Grail of PLSQL Injection.

Investigating Flaws.

Direct SQL Execution Flaws.

PL/SQL Race Conditions.

Auditing PL/SQL Code.

The DBMS_ASSERT Package.

Some Real-World Examples.

Exploiting DBMS_CDC_IMPDP.

Exploiting LT.

Exploiting DBMS_CDC_SUBSCRIBE and DBMS_CDC_ISUBSCRIBE.

PLSQL and Triggers.

Wrapping Up.

Chapter 6 Triggers.

Trigger Happy: Exploiting Triggers for Fun and Profit.

Examples of Exploiting Triggers.

The MDSYS.SDO_GEOM_TRIG_INS1 and SDO_GEOM_TRIG_INS1 Triggers.

The MDSYS SDO_CMT_CBK_TRIG Trigger.

The SYS.CDC_DROP_CTABLE_BEFORE Trigger.

The MDSYS.SDO_DROP_USER_BEFORE Trigger.

Wrapping Up.

Chapter 7 Indirect Privilege Escalation.

AHop, a Step, and a Jump: Getting DBA Privileges Indirectly.

Getting DBA from CREATE ANY TRIGGER.

Getting DBA from CREATE ANY VIEW.

Getting DBA from EXECUTE ANY PROCEDURE.

Getting DBA from Just CREATE PROCEDURE.

Wrapping Up.

Chapter 8 Defeating Virtual Private Databases.

BUY ONLINE AT: <http://www.itgovernance.co.uk/products/1249>

Tricking Oracle into Dropping a Policy.

Defeating VPDs with Raw File Access.

General Privileges.

Wrapping Up.

Chapter 9 Attacking Oracle PL/SQL Web Applications.

Oracle PL/SQL Gateway Architecture.

Recognizing the Oracle PL/SQL Gateway.

PL/SQL Gateway URLs.

Oracle Portal.

Verifying the Existence of the Oracle PL/SQL Gateway.

The Web Server HTTP Server Response Header.

How the Oracle PL/SQL Gateway Communicates with the Database Server.

Attacking the PL/SQL Gateway.

The PLSQL Exclusion List.

Wrapping Up.

Chapter 10 Running Operating System Commands.

Running OS Commands through PL/SQL.

Running OS Commands through Java.

Running OS Commands Using DBMS_SCHEDULER.

Running OS Commands Directly with the Job Scheduler.

Running OS Commands Using ALTER SYSTEM.

Wrapping Up.

Chapter 11 Accessing the File System.

Accessing the File System Using the UTL_FILE Package.

Accessing the File System Using Java.

Accessing Binary Files.

Exploring Operating System Environment Variables.

Wrapping Up.

BUY ONLINE AT: <http://www.itgovernance.co.uk/products/1249>

Chapter 12 Accessing the Network.

Data Exfiltration.

Using UTL_TCP.

Using UTL_HTTP.

Using DNS Queries and UTL_INADDR.

Encrypting Data Prior to Exfiltrating.

Attacking Other Systems on the Network.

Java and the Network.

Database Links.

Wrapping Up.

Appendix A Default Usernames and Passwords.

Index.