

Database Hacking Project

Spring 2006

Agenda

- Administration
- General Introduction to Database Network Protocols
- Tools of the Trade
- Sample Vulnerabilities
- Deeper Plunge into Database Network Protocols

Administration

- Schedule & Deliverables
- Grades
- Facilities
- Meetings

Administration

Schedule & Deliverables

- DB Installation
- Progress Report 13/04
 - Environment Status
 - General Ideas
 - Review Open Issues
- Testing Program 04/05
 - Detailed Description of Test Cases
 - What to do, how to do it, expected results
- Project Presentation 06/07
- Final Report 20/07
 - Test cases
 - Results
 - Future directions

Administration

Grades

- Test Plan
 - Originality
 - Extensiveness
 - Effectiveness
- Implementation
 - Number of tests cases accomplished
- Project Requirements
 - Schedule
 - Report format / content
 - Presentation
- Bonus
 - Findings
 - Tools

Administration Facilities

- Networking Lab – Itai Dabran
- Common Server – Windows 2K
- Two Workstations – Windows XP

Administration Meetings

- ??????????

Introduction to Network DB Protocols

- Carry commands from client to server:
 - Authentication
 - Queries
 - Control
- Designed to ride on top of session protocol (TCP, NETBIOS, etc.)
- Proprietary:
 - MS SQL: TDS 4.2,7,8
 - Sybase: TDS 4.2,5.0
 - Oracle: NET8
 - DB2: DRDA

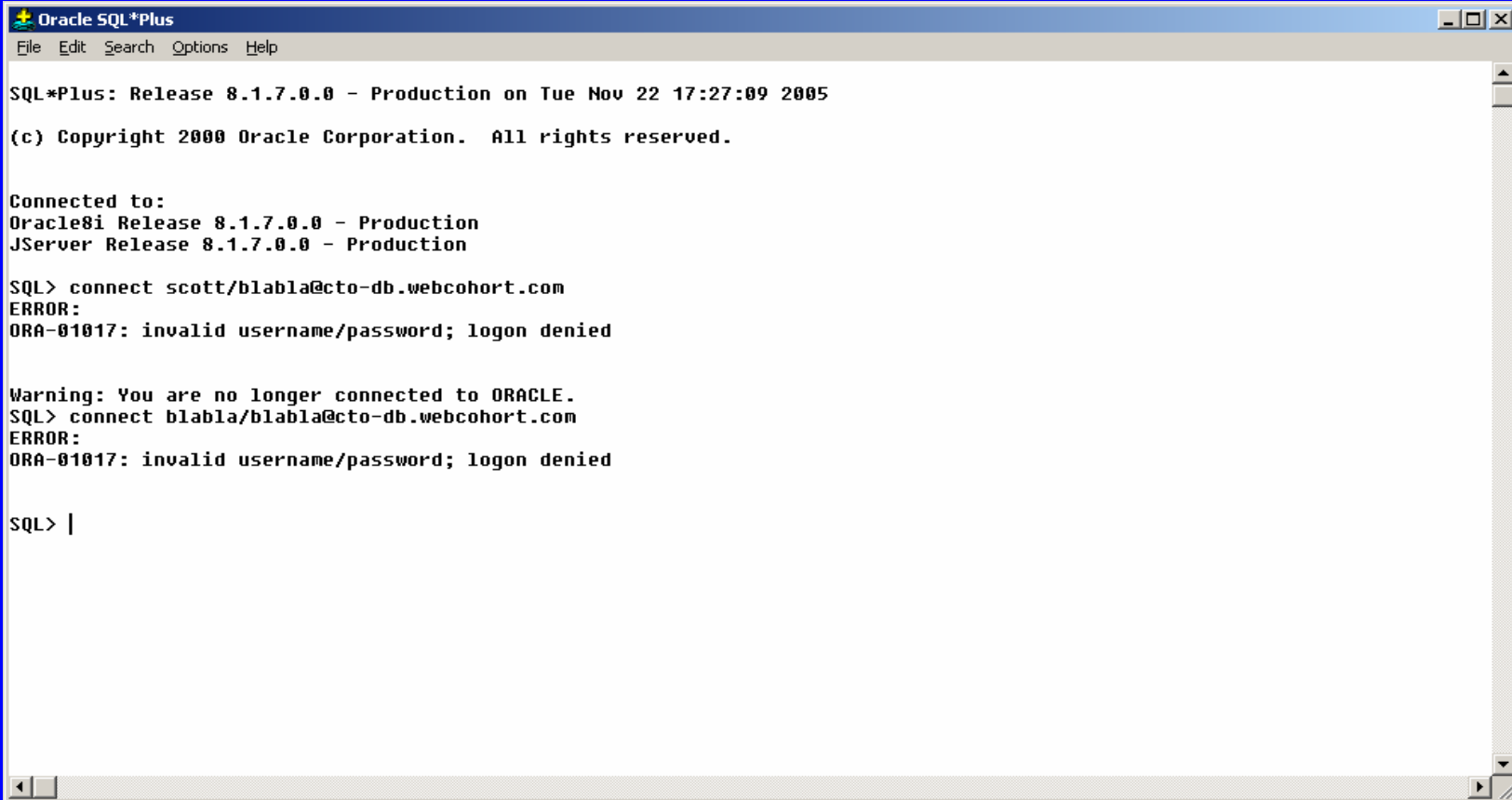
Tools of the Trade

- Ethereal
 - Monitor and capture network traffic
- Netcat
 - Stream content from file to network using TCP
- Relaytcp
 - Entry level relay for TCP traffic
- TCPirate
 - Advanced TCP hacking tool
- Hex Editor
 - Manipulate files offline

Sample Vulnerabilities

- MS SQL buffer dump
- MS SQL Evade audit
- Oracle authentication data leakage

Sample Vulnerabilities



```
Oracle SQL*Plus
File Edit Search Options Help

SQL*Plus: Release 8.1.7.0.0 - Production on Tue Nov 22 17:27:09 2005

(c) Copyright 2000 Oracle Corporation. All rights reserved.

Connected to:
Oracle8i Release 8.1.7.0.0 - Production
JServer Release 8.1.7.0.0 - Production

SQL> connect scott/blabla@cto-db.webcohort.com
ERROR:
ORA-01017: invalid username/password; logon denied

Warning: You are no longer connected to ORACLE.
SQL> connect blabla/blabla@cto-db.webcohort.com
ERROR:
ORA-01017: invalid username/password; logon denied

SQL> |
```

Sybase

General

- TDS – Tabular Data Stream
- PDU
 - 8 byte header
 - Data (Tokenized / Untokenized)

Sybase PDU Header

Offset	Size (bytes)	Title	Description
0	1	Message Type	A single byte representing the type of payload. See further details below.
1	1	Status	A bit mask that describes characteristics of the PDU. 0x01 – Last PDU in a message (EOM flag) 0x02 – Attention ACK (used for cancellation). 0x04 – Attention request (used for cancellation). 0x08 – Event notification from server. 0x20 – contents are encrypted
2	2	PDU Size	Size in bytes of the entire PDU, including the header. Format is always MSB first. Should be interpreted as unsigned integer.
4	2	Channel	If channel multiplexing is used then this is the channel number (allows multiple sessions to use the same TCP connection). Otherwise, should be 0. Should be interpreted as an unsigned integer. Format is always MSB first.
6	1	Packet Number	Should be 0 unless multiplexing is used. However we have seen some use by some clients. Should be disregarded. Unsigned integer modulo 256.
7	1	Window	Should be disregarded.

Sybase Message Types

Code	Name	Comments
0x01	TDS_BUF_LANG	Contains an SQL statement. Should be interpreted for backwards compatibility.
0x02	TDS_BUF_LOGIN	Contains a login record.
0x03	TDS_BUF_RPC	Contains an RPC. Should be interpreted for backwards compatibility.
0x04	TDS_BUF_RESPONSE	A reply message from the server
0x06	TDS_ATTN	An asynchronous client message requesting immediate attention
0x0F	TDS_NORMAL	Contains a tokenized command.

DB2

DRDA

- DRDA Version 3
- Based on “open standard”, from the people who brought us MOTIF™.
- Covered in 3 volumes of approx. 3000 pages
- Don't Panic!

DB2

DRDA – Layer A

Offset	Size	Name	Description / Value
0	2	Length	The length of the entire object including this field. Minimum is 6. The lower 15 bits are used for the length. The higher bit signals that the data stream structure is fragmented. Fragments follow immediately.
2	1	C	0xD0
3	1	Format	Stream Structure Format. Lower nibble specifies the type of object: 1 – RQSDSS object 2 – RPYDSS object 3 – OBJDSS object 5 – RQSDSS object with no expected reply This upper nibble is a bit mask with the following interpretation of bits: 4 – Chained object has same RC 5 – Continue chain processing on error 6 – Chained object follows 7 – Reserved
4	2	Request Correlation (RC) identifier	Unsigned number that identifies a request within a chain. The respective reply and object stream structure should have the same CR.
6		Data	

DB2

DRDA – Layer B

Offset	Size	Name	Description / Value
0	2	Length	The length of the entire object including this field Minimum is 4 The highest bit is off (i.e. length is smaller than 32Kbytes)
2	2	Code Point	The DDM code of the object
4		Data	

Oracle

General

- Two layers:
 - NS
 - TTI
- More than 15 year of backwards compatibility
- TTI Layer allow for multiple presentations:
 - 3 Number field representations
 - Two string data representations

Oracle

General

- NS Layer used for initial connection and streaming of data between two parties
 - Relatively simple
- TTI include database semantic
 - Complex
 - Many unexplored areas

Oracle NS Header

Type Number	Name	Description	Direction
1	Connect	Request connection from a database server	Client to Server
2	Accept	A database server accepts a connection request	Server to Client
4	Refuse	A database server refuses a connection request	Server to Client
5	Redirect	The listener process accepts a connection request and redirects it to be handled by a separate process	Client to Server
6	Data	Packets that wrap TTI messages and additional data	Client to Server Server to Client
11	Resend	The server requests a retransmit of the last packet	Server to Client
12	Marker	Synchronization signals	Client to Server Server to Client

Tips & Tricks

- Use Ethereal to capture simple sessions and analyze them, to get familiar with the structure of message
- Use www.securityfocus.com to look for previous vulnerabilities related to the protocol
- Ideas can come out of looking at implementation code. Java code implementing the various protocols is available by decompiling JDBC type 4 drivers (from vendor or from DataDirect).