Attacking and Defending Oracle
David Litchfield

www.ngssoftware.com
ATTACK || DEFENCE
PART I – PART II
Part I: The Attacks

Information Gathering
  Listener
  User Enumeration

Gaining Control
  Command Insertion via Trace/Log files
  LoadLibrary/Extproc
  Extproc Buffer Overflow
<table>
<thead>
<tr>
<th>Information Gathering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
</tr>
<tr>
<td>Platform</td>
</tr>
<tr>
<td>SIDs</td>
</tr>
<tr>
<td>Ports</td>
</tr>
<tr>
<td>Configuartion</td>
</tr>
<tr>
<td>Done through the Listener</td>
</tr>
</tbody>
</table>
The Oracle Listener

- RDBMS
- Extproc
- Registration
- Deregistration
- PL/SQL
- Client Connections
LSNRCTL Utility

STATUS Command
SERVICES Command
VERSION information
(VSNNUM=153092352)
HEX = 9200100
User Enumeration

Much like VRFY with SMTP – guess work.

Valid User – SESSION_KEY
Invalid User – no SESSION_KEY

If auditing of CREATE SESSION is enabled even if connection is terminated before completion attempt is still logged!
Command Insertion
Using the lsnrctl

Set the logfile to script that will be executed such as administrator’s startup folder then issue command.

```
set log_status on
set log_file c:\autoexec.bat
```

Insert command - &
```
set log_file c:\old_log_file.log
```
LoadLibrary/Extproc

External Procedure call from PL/SQL

Oracle -> Listener
Listener launches EXTPROC
Listener -> Oracle
Oracle -> EXTPROC

Fixed in 9.2
Must be local.

Library must be in the `${ORACLE_HOME}` directory.
Problems:

Local attacks still possible.

Directory traversal.

Remote attempts are logged.
The fix is BROKEN.

Whilst logging the attempt and overflow occurs.

So we can still gain control without a USERID and PASSWORD.
Part II: The Defence
Set a Listener password.

Set ADMIN_RESTRICTIONS to ON.

Remove entries in listener.ora and tnsnames.ora for Extproc.
Use tcp valid node checking

Ensure file permissions are strong.

Enable auditing of CREATE SESSION.
Run as a low privileged user.

PATCH!
Questions?
Thanks for coming!