Attack your Oracle database to make it more secure

OGh DBA en SQL Celebration Day, June 2016

Andre van Winssen, 7 Juni 2016

Who am I

Andre van Winssen
Principal Oracle Consultant @ Amis
Previously: Shell IT, Oracle Support NL
OCP 7.3, 8i, OCM 10g, 11g, 12c
CISSP-ISSAP, CISA
(Newbie) grandpa

- Databases
- RAC
- Performance
- Security
- Weblogic
- Audits

andre.vanwinssen@amis.nl

https://nl.linkedin.com/in/andrevanwinssen

https://technology.amis.nl/

Agenda

- **Information security & Risk management**
- Status quo
  - Map of Public Vulnerability to Oracle Advisory/Alert (What's in latest Oracle's CPU's? **)**
  - Exploits available in the wild
  - Exploits privately held
- Database attack tooling
  - ODAT, MSF, OPENVAS,
  - SQLPLUS
  - Oradebug
  - ..
- Where to go from here

Information security

- What is confidentiality, integrity, (availability)?
- EU Data Protection Regulation
- Where are the CI(A) data elements in my database
  - that come with an Oracle's own CI(A) database
  - that my application developers created
- Do we comply to our own business access policy and how to find out?

EU Data Protection Regulation

- German Data Protection Act (BDSG)
- Accountability
- Data Protection along the lifecycle of products and processes (Article 25)
- Principle of data minimisation (Article 5)
- Storage limitation (Article 5)
- Duty to implement data security (Article 32)
- Data breach notification to the authority (Article 33)
- Data breach notification to the data subject (Article 34)
- Proposed network and information security directive (Article 14)

Agenda

- Information security & Risk management
- **Status quo**
  - Map of Public Vulnerability to Oracle Advisory/Alert (What's in latest Oracle's CPU's? **)**
  - Exploits available in the wild
  - Exploits privately held
- Database attack tooling
  - ODAT, MSF, OPENVAS,
  - SQLPLUS scripts
  - SQLPLUS' oradebug
  - ..
- Where to go from here

Map of Public Vulnerability to Advisory/Alert

Vulnerability Identifier	Advisory
CVE-2011-4461	Oracle Critical Patch Update April 2016
CVE-2013-2566	Oracle Critical Patch Update April 2016
CVE-2013-4786	Oracle Critical Patch Update April 2016
CVE-2014-2532	Oracle Critical Patch Update April 2016
CVE-2014-3566	Oracle Critical Patch Update April 2016
CVE-2014-3576	Oracle Critical Patch Update April 2016
CVE-2015-1789	Oracle Critical Patch Update April 2016
CVE-2015-1790	Oracle Critical Patch Update April 2016
CVE-2015-1793	Oracle Critical Patch Update April 2016
CVE-2015-1794	Oracle Critical Patch Update April 2016
CVE-2015-2721	Oracle Critical Patch Update April 2016
CVE-2015-2808	Oracle Critical Patch Update April 2016
CVE-2015-3193	Oracle Critical Patch Update April 2016
CVE-2015-3194	Oracle Critical Patch Update April 2016
CVE-2015-3195	Oracle Critical Patch Update April 2016
CVE-2015-3196	Oracle Critical Patch Update April 2016
CVE-2015-3197	Oracle Critical Patch Update April 2016

>3220 entries since with oldest from january 2010.

The entry creation date (e.g. 20111117) may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Exploits available in the wild

- See websites of people like
  - David Litchfield
  - Pete Finnigan
  - Paul Wright
  - Laslo Toth
  - Tanel Poder
- https://nmap.org/nsedoc/scripts/oracle-...
- ...

Exploits privately held

- Used by 3 G's: *gangsters, governments, geeks*
- Worth a lot of money
- Breaching databases without defense(?)
- Unknown owners, traders
- Not likely to be listed in any vulnerability database

Agenda

- Information security & Risk management
- Status quo
  - Map of Public Vulnerability to Oracle Advisory/Alert (What's in latest Oracle's CPU's? **)**
  - Exploits available in the wild
  - Exploits privately held
- **Database attack tooling**
  - ODAT, MSF, OPENVAS,
  - SQLPLUS scripts
  - SQLPLUS' oradebug
  - ..
- Where to go from here

Database Attack tooling

- To name a few
- ODAT – Oracle database attack tool
- Metasploit Framewerk (msf)
- OpenVAS (vulnerability assessment tooling)
- Sqlplus scripts
  - From Password hash to cleartext
  - Privileges lists
  - Privilige elevation (remember Baron von Munchhausen)
  - oradebug

Agenda

- Information security & Risk management
- Status quo
  - Map of Public Vulnerability to Oracle Advisory/Alert (What's in latest Oracle's CPU's? **)**
  - Exploits available in the wild
  - Exploits privately held
- Database attack tooling
  - ODAT, MSF, OPENVAS,
  - SQLPLUS scripts
  - SQLPLUS' oradebug
  - ..
- **Where to go from here**

Where to go from here – some advise

- Use non-oracle supplied roles
- Remove ANY privileges
- Beware of dangerous
- Use smart AUDITing (FGA!)
  - Audit only relevant events
  - Use it to do privlege analysis (don't need DBV license)
- Install compliance checking tools
- Use oracle encryption for data in transit
- Use strong authentication where possible
- Basic security
- Or if you have money to spend go for:
  - Database vault
  - Database firewall
  - Audit vault
  - Key Vault
  - Advanced Security option
    - TDE ..

amis.nl