ORACLE FORENSICS IN A NUTSHELL 25/03/2007

The aim of this paper is to summarize Oracle Forensics in a time efficient manner as follows.

1.0 Definition
2.0 Process Methodology
3.0 Core technical tasks and Techniques used
4.0 Main Sources of evidence
5.0 Legal Context
6.0 Conclusion

Recommended prior and supporting reading:
http://www.cl.cam.ac.uk/~rja14/book.html
http://philip.greenspun.com/sql/
http://www.porcupine.org/forensics/forensic-discovery/
http://www.sleuthkit.org/
http://www.e-fense.com./helix/
http://cuddletech.com/articles/oracle/index.html
http://www.sans.org/score/oraclechecklist.php

1.0 DEFINITION

"Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system." Farmer and Venema, 1999.
http://www.porcupine.org/forensics/forensic-discovery/appendixB.html

2.0 PROCESS METHODOLOGY

Principles:

1. Documented processes to produce repeatable results
2. Best evidence for court i.e. analysis done on the copy
3. Chain of custody implemented to enforce evidence accountability

Process:

1. Initiate a documented timeline of computer based events
2. Identify and contain the incident
3. Back up electronic files as evidence in chain of custody
4. Recover service and deleted data
5. Collecting and sorting electronic metadata by time
6. Integrate all event information into the timeline which includes log aggregation
7. Analysis of metadata timeline
8. Detailed examination of key data at lower level
9. Document the process to make findings repeatable
10. Apply the evidence to a criminal or legal context

3.0 CORE TECHNICAL TASKS AND TECHNIQUES USED

1. **Backing up evidence in a verifiable way using checksums, file size and timestamps.**

At the OS:

Start netcat listener on forensic_host to capture an image

```
#nc -l -p 33333 > /tmp/driveimage.dd
```

Use dd to collect image and netcat to send it across the network

```
#dd if=/dev/hda2 | nc host 33333 –w 3
```

Can check integrity using md5sum on a drive or bit image file

```
# md5sum /dev/hda1
```

In the DB:

1. RMAN

http://www.oracle.com/technology/deploy/availability/htdocs/rman_overview.htm

2. Full logical export

$ORACLE_HOME/exp "sys/password as sysdba" full=y file=export.dmp

3. Cold backup ~ offline

```
cp /oracle/oradata/SID/*.dbf  /oracle/oradata/clone/
cp /oracle/oradata/SID/*.log  /oracle/oradata/clone/
cp /oracle/oradata/SID/*.ctl  /oracle/oradata/clone/
```

4. Hot backup ~ online

```
alter tablespace data begin backup
alter database backup controlfile to c:\backupcontrolfile.bak
```

5. Verify

```
dbv file=c:\oracle\datafile.bak logfile=C:\dbverifylog
```

2. **Recovering deleted data such as that which an attacker may have attempted to hide.**

At the OS:

To recover deleted files from Linux OS. This script requires installation of The Coroners Toolkit from http://www.porcupine.org/forensics/tct.html

```
# ils –rf linux-ext2 /evidence/driveimage.img | \
 awk –F '|' '($2=="f") {print $1}' | \
 while read i; \
 do /usr/local/src/sleuthkit/bin/icat -f linux-ext2 \
 /evidence/driveimage.img $i > \
 /deletedfiles/$i; \
 Done
```

http://project.honeynet.org/scans/scan15/proj/t/analysis-scan-may-2001.txt

Foremost will carve out files based on their headers.

```
#foremost -v -c foremost.conf ext2binarycopy.dd
```

http://sourceforge.net/projects/foremost/

At the DB:

Flashback

select ora_rowscn, name from sys.user$;

SELECT To_Char(TIME_DP,'dd/mm/yyyy hh24:mi:ss'), SCN_BAS FROM SYS.SMON_SCN_TIME;

```
FLASHBACK TABLE SQUIRRELPATCH TO SCN 2202666520;
```

Redo Logs using LogMiner

http://www.giac.org/certified_professionals/practicals/gcfa/0159.php

http://orafaq.com/papers/redolog.pdf

3. In depth data analysis entailing lower level inspection of data than normal

At the OS

Hexedit, WinHex forensic version http://www.x-ways.net/winhex/forensics.html Ethereal hexadecimal network packet analyzer, Ultra-Edit binary editor. http://home.online.no/~espensa/khexedit/

DUDE or JDUL allows examination of Oracle datafiles that would not normally be possible http://www.ora600.nl/introduction.htm

Can use BBED http://orafaq.com/papers/dissassembling_the_data_block.pdf

or directly analyse the dbf's themselves.

http://www.oracleforensics.com/wordpress/index.php/2007/03/21/dbf-records-previous-state-of-each-row/

At the DB

Oradebug see
http://julian.dyke.users.btopenworld.com/Oracle/Diagnostics/Tools/ORADEBUG/ORADEBUG.html

Ian Redfern's TNS protocol analysis
http://www.ukcert.org.uk/oracle/Oracle%20Protocol.htm

Pete Finnigan's PLSQL unwrapping

http://www.insight.co.uk/files/presentations/BlackHat%20conference.pdf

All of the above allow the analyst to understand what is happening in Oracle which is required to be able to make judgements about electronic evidence with a high level of certainty.

In terms of analysing the actions of an attacker a good understanding of Oracle attacks is crucial therefore the Oracle Hacker's Handbook would be a good read so that the forensics analyst knows what to look for.

http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470080221.html

4. **Timeline analysis by placing evidence on a timeline to show order of past events.**

At the OS and at the DB!

Create a body file using this command.

```
# fls -f linux-ext2 -m / -r /driveimage.img > /driveimage.fls
```

Other datafiles can be parsed into the body file. Then use mactime perl script to sort the entries by timestamp. Mactime is part of the Sleuthkit.
http://www.sleuthkit.org/sleuthkit/man/mactime.html

mactime -b /bodyfile/body.mac >/bodyfile/body.all

MACtimes = Modified, Accessed and Changed times.

Problem is that the timestamps could have been changed therefore need to keep logs off the server being protected on a secure central loghost. This can be done more easily with Oracle now by utilising its SYSLOG functionality.

```
ALTER SYSTEM SET audit_trail=OS SCOPE=SPFILE;
SQL> ALTER SYSTEM SET audit_syslog_level='USER.ALERT' SCOPE=SPFILE;
System altered.
```

Syslogger download
http://bent.latency.net/bent/darcs/minirsyslogd-1.02/src/minirsyslogd-1.02.tar.gz

Installing the remote syslog host using these links.
http://bent.latency.net/bent/darcs/minirsyslogd-1.02/spec

vi /etc/syslog.conf and configure syslog as normal.
http://www.linuxjournal.com/article/5476

Place the sources of evidence from the next section onto the Depository loghost along with the SYSLOG basic Oracle audit and then create a timeline using external tables to query the logs using one SQL VIEW which uses TIMESTAMP as both foreign and primary key. It will be useful to measure TIMESTAMP to a higher decimal place precision so that the primary key timestamps stay unique. This is an example of mapping a listener logfile to db table for SQL.

```
create directory LISTENERDIR
   as '/u01/app/oracle/oracle/product/10.2.0/db_4/network/log'
   /
   create table listenerlog
   (
      logtime1 timestamp,
      connect1 varchar2(300),
      protocol1 varchar2(300),
      action1 varchar2(15),
      service1 varchar2(15),
      return1 number(10)
   )
   organization external (
      type oracle_loader
      default directory LISTENERDIR
      access parameters
      (
         records delimited by newline
         nobadfile
         nologfile
         nodiscardfile
         fields terminated by "*" lrtrim
         missing field values are null

         (
```

```
            logtime1 char(30) date_format
            date mask "DD-MON-YYYY HH24:MI:SS",
            connect1,
            protocol1,
            action1,
            service1,
            return1
         )
      )
      location ('listener.log')
)
reject limit unlimited
/
```

Marcus Ranum and Tina Birds site at http://www.loganalysis.org/ is good for log analysis. Time synchronisation is key to the accuracy of timelines created. Refer to http://www.ukcert.org.uk/time_security.html for more detail. For detailed information on creating a Depository consult my Oracle Forensics book from http://www.rampant-books.com and this URL in the future www.oracleforensics.com/depository.html

4.0 MAIN SOURCES OF EVIDENCE

1. Listener log – logs connections to the listener, use lsnrctl to administrate it. Can be found in `/u01/app/oracle/oracle/product/10.2.0/db_4/network/listener.log`
2. Alert log – system alerts important to DB e.g processes starting and stopping. Can be found in `/u01/app/oracle/admin/orcl/bdump`
3. Sqlnet.log – some failed connection attempts such as “Fatal NI connect error 12170”.
4. Redo logs - current changes that have not been checkpointed into the datafiles (.dbf).

   /u01/app/oracle/oradata/orcl/redo02.log

   /u01/app/oracle/oradata/orcl/redo01.log

   /u01/app/oracle/oradata/orcl/redo03.log
5. Archived redo logs – previous redo logs that can be applied to bring back the data in the db to a previous state using SCN as the main sequential identifier. This can be mapped to timestamp.
6. Fine-Grained Auditing audit logs viewable from FGA_LOG$ and DBA_FGA_AUDIT_TRAIL VIEW.
7. Oracle database audit SYS.AUD$ table and DBA_AUDIT_TRAIL VIEW.
8. Oracle mandatory and OS audit `/u01/app/oracle/admin/orcl/adump`
9. Home-made trigger audit trails - bespoke to the system.
10. Agntsrvc.log – contains logs about the Oracle Intelligent agent.
11. IDS, Web server and firewall logs should also be integrated to the incident handling timeline. This will rely heavily on well synchronised time in the network as previously mentioned.

5.0 LEGAL CONTEXT

The experience passed on to me by Forensic expert witnesses is that the main challenge lies in translating the technicalities of an analysis to the level of understanding held by the court officials and jury. This can be overcome by use of demonstrations and simplified examples. The other main challenge is placing the evidence and analysis results correctly in their legal context which requires the collaboration of legal and technical minds. The more that each know of the two subject areas the more effective this collaboration, therefore below are listed the main laws and standards that will affect Oracle Forensics cases in the future in the US.

Computer Fraud and Abuse Act, 18 U.S.C. §1030 - Network Crimes
Wiretap Act, 18 U.S.C. §2511 - Wiretapping and Snooping
Privacy Act, 18 U.S.C. 2701 - Electronic Communications
Sarbanes Oxley section 404 – enforce financial standards to limit chance of fraud. http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/
HIPAA – see Oracle Privacy Auditing Donald Burleson & Arup Nanda. http://www.dba-oracle.com/bp/bp_book11_audit.htm and http://www.cms.hhs.gov/hipaa/
Fair Credit Reporting Act (FCRA) limits use and distribution of personal data, and allows consumers to access the information held about them, though it only applies to information primarily used to make eligibility determinations http://www.gao.gov/new.items/d06674.pdf
Graham Leach Billey - http://banking.senate.gov/conf/grmleach.htm requires disclosure of privacy policies to customers and financial standards in general. These policies should restrict the passing on a non-public personal information and requires this information to be safeguarded.
Financial Anti-Terrorism Act (H.R. 3004) of 2001 as part of the Patriot Act.
Basel II – Stipulates a relationship between the risk assessed for a bank and the amount of capital that needs to be set aside to balance that risk. Therefore Basel II provides a financial incentive for banks to reduce risk.
SB 1386 California Data Breach act
New York Data Breach act – NY version of SB1386
PCI Credit card security standard requires installation of patches https://sdp.mastercardintl.com/pdf/pcd_manual.pdf "6.1.1 Install relevant security patches within one month of release." Also should be encrypted credit card details in the db. https://www.pcisecuritystandards.org/tech/index.htm
Data protection act 1998 UK and similar acts globally as referenced by the Safe Harbor Act http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm http://www.export.gov/safeharbor/ .

Expert legal advice can be sought from http://richardsalgado.home.att.net/instructors.htm

6.0 CONCLUSION

This paper has summarized the field of Oracle Forensics to give a time efficient overview of the subject. For a more in-depth description then Oracle Forensics by the Author Paul M. Wright http://www.rampant-books.com/book_2007_1_oracle_forensics.htm should be consulted along with this website www.oracleforensics.com . Feedback to paul.wright@oracleforensics.com

The paper will be updated over time at http://www.oracleforensics.com/summary.html