Q1/7

In SQLMap if we want to extract databases, we use -dbs switch.

A True

B False

Well done. Correct Answer.

Explanation:
We use --dbs (double hyphen). All switches which have single letters like -T -C -D are used with one hyphen and when the switch has more than one letter, 2 hyphens are used example --tables --columns --dbs. Also, in place of space, a lot of times developers use another hyphen. Example --is-dba.

Q2/7

When we use sqlmap to test for Blind injection and Error Based injection what is the command we use?

A	--technique BS
B	--technique UE
C	--technique BE

Well done. Correct Answer.

Explanation:
We use --technique BE to search for Boolean based injection and Error based injection The abbreviations are: B - Boolean E - Error U - Union S - Stack Query T - Time based Q - Inline query injection So if you want to force injection using union, you can specify --technique U. Tip: You can also increase the level of intensity by giving --level 3.

Q3/7

-T switch is used for which of the following purposes?

A Get all table names

B Specify which table to get information from

Well done. Correct Answer.

Explanation:
--columns is used to get all the columns, --tables is used to get the table names, but to get all columns in a particular table we can use --columns -T “specific table name”.

C Specify the number of the threads to execute

D None of the above

Q4/7

If we want to dump all the databases, tables, and entries inside them, which of the following commands can be used?

A --dump

B --dump-all

Well done. Correct Answer.

Explanation:
If we want to dump a single database table entry we use --dump whereas if we want to dump all the data in the server we use --dump-all. Do note that this will take a lot of time especially if the injection type is not Union.

C --dump-tables

D None of the above

Q5/7

In SQLmap --threads switch is used for which of the following purposes?

A To increase the level of complexity

B To increase the risk level

C To increase the speed of the attack

Well done. Correct Answer.

Explanation:
--threads switch is used to increase the speed of the attack using multi threading, for example: --threads=10 --level=1/2/3 can be used to change the level of the attack --risk=1/2/3 can be used to try more dangerous payloads to test for SQL injections.

D All of the above

Q6/7

In SQLmap if we want to try a fresh query by flushing the session files for the target, which of the following switches will be used?

A --fresh-queries

B --flush

C --flush-session

Well done. Correct Answer.

Explanation:
In sqlmap --fresh-queries switch is used to ignore query results stored in session file and --flush-session is used to flush the session files for the target.

39% students get this answer correct at their first attempt

D All of the above

Q7/7

You want to do SQL injection in User-Agent header by saving the file and using SQLmap's -r option. You right click on the request in burp and copy the request to a file sql1.txt. You now open the file with notepad and want to specify sqlmap to inject right after the header: User-Agent: Mozilla 30..... [HERE] Which character do you put at this place?

A	$HERE$
B	%
C	*here*
D	* ✓

Well done. Correct Answer.

Explanation:
To inject at a specific point, put a * in the request, pass the request's file to sqlmap using sqlmap.py -r sql1.txt and when sqlmap asks that "do you want to test on custom locations pointed by *" select yes.

Now that we have come to the end of this topic, you should be able to:

1. Explain SQLMap.
2. Install and setup Python and SQLMap in their systems.
3. Automate SQL testing in GET based parameters.
4. Automate SQL testing in POST based parameters.
5. Understand Authenticated SQLi and exploit them using Burp Suite and SQLmap.

If you have doubts regarding any of the above mentioned points, please go through the relevant videos and text chapters again.