**INFS3617 Networking & Cyber Security**

Sandbox Weekly Reflection

| | |
|---|---|
| **Name:** Bevan Lui | **zID:** z5160501 |
| **Tutorial Week and Date:** Week 9, Friday 11am, 17/4/2020 | |

Explain TWO networking and/or cyber security concepts you have learned in your lab this week. Your description should be in the format provided below:

*(**1.1**) Activity 3 Injection (SQL)*

Using SQL Injection to log in as an administrator

***(1.2)***

SQL injection involves using queries to send untrusted data to an interpreter to access data or execute commands without the need for authorisation. SQL injections are used to query a database to retrieve or write data to tables, by using SQL injections an attacker can make an interpreter evaluate a statement to be TRUE, to access database records. In the activity we used 'OR "**1=1; --**" to login as administrator without the need for a password. The "1=1" tricks the query to evaluate to always be true, the '--' means a comment in SQL, by doing this the SQL injection eliminates he password validation which allows us to login as the first record in the table, in this case admin. SQL injections and injections in general only work when there are errors in implementation, so in the activity having prepared statements would've prevented the SQL injection attack to work.

*(**2.1**) Activity 4 Hashing - Hashcat*

Using hashing to check for passwords

***(2.2)***

Hashing maps data of random size to fixed size data or to obscure data in the activity for passwords in the database. Hashcat is a password recovery tool using algorithms and patterns to crack hashed passwords. In the activity by using a previous SQL query the hashed passwords can be extracted and saved in a textfile that will be run on hashcat to discover the passwords. Hashing can take a long time, however in cases of a weak hash, where there haven't been repeated hashing or salt passwords, where random data is added, it will be quick to complete the hashing. On hashcat by using a dictionary it can further quicken to process by looking for passwords with only real words, this is what happened in the activity by using a dictionary the process was sped up and returned results. Otherwise without the dictionary it would've taken a much longer time because there was nothing to look for only to use algorithms from hashcat to find passwords.