Assignment Week

Network Security

MOULINNEUF Galdan - 2927686

Question 1 :

Decrypted Caesar cipher – key = 10

a) It would be better to use the second strongest password (P4sswOrdOn3!) because it's pretty secure thanks to the lenght, upper character, lower character, numbers an special characters. Futhermore, it's easier to remember than the strongest (This20is21my22Passphrase23!!24).

   The compromise here is that a human will be more likely to remember the second strongest and still be very secure.

b) To bruteforce the password number one (Password1), we need to determinate the key space which will be composed of the basic Ascii.

   So it twill take 2^8 = 256 hours to brute force it. It takes not much because the encryption is base on a one byte encryption. To renforce it, we make several bytes encryption.

Question 2 :

Decypted Rail Fence cipher – key = 5

a) Here is the ten-step process for security policy implementation :

1. Evaluate the risk
2. Establish a monitoring strategy and supporting policies
3. Monitor all ICT systems
4. Monitor network traffic
5. Monitor all user activity
6. Test legal compliance
7. Fine-tune monitoring systems
8. Establish a centralised collection and analysis capability
9. Train the security personnel
10. Align the incident management policies

b) A risk assessment would be useful because establishing a security policy can cost lot of money AND time. A risk assessment will inform you that at some point of your network, it will cost you more, in term of money and time, to implement a policy rather than lost them.

Question 3 :

Decrypted Vigenere Cipher – key = cake

a) The number assigned to it describes the protocol that this list is managing.

b) Similiarities between an ACL and a Firewall is the way they let/don’t let traffic going and where they are place in a network structure.

c) The list that will allow telnet to any host is :

« A. 140 permit tcp any any eq 23 log »

Question 4 :

Decrypted Column Shift Cipher – Key = « 3 5 1 6 7 2 4 »

a) The following are MD5 :

- 1. 8fc42c6ddf9966db3b09e84365034357
- 3. a2a551a6458a8de22446cc76d639a9e9
- 6. eb0c28768b1cfe1c105a8c7a2484dd57

b) The Caesar code is decrypted with a key of 3.
It gives us this decrypted text : « MARY HAD A LITTLE LAMB ».
Removing punctuation, spaces and in lower case gives : « maryhadalittlelamb ».

Hashed, this sentence is : ad6504a4eafcea51d049b466c1ed869d0ada1ca1, which doesn't match with any in the list.