UNIT 1.6 test SOLUTIONS

#whydoesthisfeelfamiliar
#thisisjustmicrotest10again

1) Describe what the term phishing means [2]
Use of emails or texts claiming to be well known businesses (eg a bank or retailer) asking user to update their personal information. Usually include links to spoof versions of the real sites. Allows criminals to get hold of your official account details.

2) Describe using an example what is meant by social engineering [2]
A way of gaining sensitive information or illegal access to networks by influencing people, usually the employees of large companies. Usually over the telephone, gaining trust from an employee is order to persuade them to give up confidential information. For example claiming to be a network administrator.

3) Describe what a denial of service attack is [2]
Where hackers try to stop users from accessing a network or website through flooding the network with useless traffic. The makes it extremely slow or completely inaccessible.

4) Explain the concept known as SQL injection [3]
Where SQL code is typed into input boxes on a website to expose vulnerabilities in the way it has been coded. For example you may need a PIN number to enter a site. An SQL attack on a poorly designed input box could be "SELECT name, account number WHERE pin = 12345 OR 1=1". Since 1=1 is always true this could then provide all customer names and account details to the hacker. Exploits validation weaknesses in databases via web forms.

5) Identify 3 features that would keep a password effective [3]
Minimum length, alphanumeric, capital letters, symbol use, nonsense term, changed regularly

6) Describe what is meant by penetration testing [2]
Where organisations employ specialists to simulate an attack on the network. They then publish a report on potential weaknesses so that they can be addressed.

7) Describe what is meant by network forensics [2]
Are investigations undertaken to find the cause of an attack. Requires capturing of data packets on the network so that they can be analysed. This information is used to prevent future attacks.

8) Identify 2 things you would find on a network policy [2]
No use of social networking sites, no inappropriate/offensive web content, no video streaming etc…

9) Describe the role of a firewall on a network [2]
To monitor and manage all inbound and outbound communications to the network. Blocks and opens ports. Has a list of authorised programs.

10) Describe the term encryption [2]
Scrambling the original data with a cypher key so that it is unrecognisable if intercepted. The cypher key is needed in order to decipher the data back into its original format.

11) Describe what is meant by a brute force attack to a network [2]
Usually used to crack passwords. Automated software producing hundreds of password variations with usernames to gain unauthorised access to a network. Simple locking of accounts after a few tries can prevent a brute force attack being effective.

12) Identify one form of physical security you could use to deter threats to a network [1]
Guards, CCTV, locked doors etc…