01.1 Define the term 'pharming'.

[2 marks]

Any of: A cyber attack [1] redirects web traffic [1] to fake website that looks like the original [1] to trick users into entering personal data [1]

01.2 Social engineering is where someone is tricked or manipulated into providing secure information or access to a secure system. Describe **one** of the following social engineering techniques.

- Blagging:
- Phishing:
- Shouldering (or shoulder surfing):

[3 marks]

2 marks for describing **one of** the social engineering technique.
Blagging: where a victim is tricked/persuaded (by a fraudster) to give their details or payment information (for a fraudulent reason/purpose);
Phishing: Is where the victim receives and responds to a communication that appears to be from a valid or known source (but is in fact fraudulent. It allows the fraudster to capture private information before the victim realises);
Shouldering: Where someone watches and records\remembers a victim entering their pin or security information such as passwords

01.3 Penetration testing can be conducted in **two** ways. Explain the difference between the two types of penetration testing.

[4 marks]

Maximum of 3 marks if only1 type of testing.

External attack testing:

- the tester does not know how the system operates or have any login credentials;
- the tester is acting as an external hacker;
- requires a lot of investigation and guessing/brute-force to find issues;
- may not test all of the system especially if you do not know it's full functionality;
- you are trying to discover and exploit the weak spots in the system;

Malicious insider testing:

- the operation of the system is known with the possibility of some login credentials;
- the tester is simulating a malicious insider;
- can be targeted to test specific vulnerabilities;
- you know exactly what you are trying to test;
- because you know what you are testing you should be able to test all possible scenarios;