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 each of the following social engineering techniques.

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

[3 marks]

1 mark each for describing 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 as either black-box or white-box testing. Explain the difference between these two types of penetration testing.

[4 marks]

Maximum of 3 marks if only1 type of testing.
Black box testing:

- the tester does not know how the system operates;
- 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;

White box testing:

- the operation of the system is known;
- 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;

02 A virus is a specific category of malware.
Describe two other different categories of malware.

[4 marks]

1 mark each for stating, 1 mark each for describing. Accept any reasonable method.
Trojan (horse); a program which misleads the user into thinking it is another piece of software which, when run, executes another program;
Spyware; a program which records data such as usernames and passwords on a host system and forwards the information to a third party;
Ransomware; a program that encrypts user's data to make it unreadable until they pay for the key;
Keylogger; a program that monitors/records a user's keystrokes in order to steal passwords/confidential details;.

03 A company has decided to move its business online but it is concerned about making sure that only authorised users can gain access to the system. The company has set up a CAPTCHA system to check that the user is not a robot.
Explain **three** different electronic methods other than CAPTCHA that could then be used to confirm user identity.

[6 marks]

2 marks per method, 1 mark for stating the method, 1 mark for an explanation.
Passwords; a set of characters that is only known by the person who is being authenticated// a set of characters that is entered and compared against a database/recorded version;
Biometric; measures such as fingerprint, facial, iris, voice-print that use the user's physical features to prove who they are;
Email confirmation; sends an email which requires a valid email address and for the recipient to respond to prove the email and hence user is valid;
Accept other methods that are not in the specification that are appropriate should also be awarded marks. Examples such as 2 Factor Authentication (2FA), Authenticator Apps, security questions.

04 Explain how each of the following cyber security threats could be used by a student to gain unauthorised access to a school network:

- weak and default passwords
- misconfigured access rights
- removable media
- unpatched and/or outdated software.

In your answer you should also describe some possible consequences of these threats.

[8 marks]

Level 4 (7-8 mks): detailed, well structured response dealing with all four methods. At least one consequence mentioned
Level 3: (5-6 mks): detailed explanation of how most of the threats could be exploited, making clear reference to a school network. At least one consequence mentioned
Level 2 (3-4 mks): some explanation of most of the threats with some reference to a school network. May not have referred to consequences
Level 1: some description f at least one of the threats and/or consequences