

**Group A**

Q1

output array has capcity of 15 chars, initially 9 occupied (including null terminator). data string could be be at most 10 characters (including null). So their concatenation can create a string of 18 characters, which exceeds capacity. Hence strcat() call is vulnerable.

*For full marks, they need a precise analysis like above.*

Q2

Encrypted malware encrypts its body with a random key and places a decryption routine at the start. Multiple samples of encrypted malware will all have a common code (decryptor) at the start, hence a signature can be recorded for easy identification.

Polymorphic malware is actually an encrypted malware, except that the decryption routine is differently mutated for each sample so that creating a signature is much more harder.

Q3

To send the injected SQL code to database server, attacker uses the same path as used by typical user inputs.

**Group B**

Q1

↑

Stack growing backwards

|  |
| --- |
|  |
|  |
| x = 5 |
| old frame pointer |
| func3 return address |
| address of str1 |
| a |
| b |
| c |
| null |
|  |

*They can also draw it inverted, growing downwards. Order of the items inserted is important.*

Q2

Worms exist standalone, auto injected into victim systems due to security vulnerabilities

Trojans are disguised inside apparently useful programs. Require user action to get into a target system.

Q3

Attacker’s SQL contains a condition that always evaluates to true, causing extra data to be leaked in query results.