# Module 5 / Unit 1 / Security Concerns

1. **Which property of secure information is compromised by snooping?**

Confidentiality—keeping information disclosure restricted to authorized persons only.

1. **An attacker has used a rogue access point to intercept traffic passing between wireless clients and the wired network segment. What type of attack is this?**

This is typical of a Man-in-the-Middle (MitM) attack.

1. **What type of access mechanism is MOST vulnerable to a replay attack?**

Use of a token generated by software. If the token is not authenticated properly by the server, it could be vulnerable to replay, where someone else obtaining the token can masquerade as the original user.

1. **Which specific attack uses a botnet to threaten availability?**

Distributed Denial of Service (DDoS).

1. **In considering availability concerns, what use might a lockable faceplate on a server-class computer be?**

It may prevent the user switching the machine on or off (useful for servers) or accessing removable drives and ports.

1. **What does AAA stand for?**

Authentication, Authorization, Accounting.

1. **Why should a security policy instruct users not to reveal their password to technical support staff?**

It exposes users to social engineering attacks to gather login credentials for malicious use. Any request for a password should be treated by users as suspicious.

1. **How might someone masquerade as someone else when using email or Instant Messaging?**

By accessing their user account—this could be done by stealing their login information, using an unattended computer that was still logged in, or using malware such as a Trojan.

1. **What are the three main areas where redundancy should be provisioned?**

Data/storage (RAID), network links, and power. You might additionally mention site-level redundancy, though this is very expensive to provision.

**Module 5 / Unit 2 / Using Best Practices**

1. **Part of host hardening is to reduce the attack surface. What configuration changes does reducing the attack surface involve?**

Removing unwanted and unnecessary software, disabling unused OS features and services, and closing unnecessary network ports. This reduces the ways other hosts or processes can interact with the hardened host.

1. **What is the main difference between virus and worm malware?**

A virus has to infect a file whereas a worm propagates in memory and over computer networks.

1. **How might malware hosted on a website be able to infect your computer simply by your browsing the site?**

By exploiting a vulnerability in software installed on your computer (a fault or "exploit" in the browser, a browser plug-in, or the OS for instance).

1. **How might spyware be able to steal a password?**

Typically by monitoring key strokes (a key logger). It might also be able to steal password databases and decrypt them.

1. **What type of malware is being described? The malware encrypts the user's documents folder and any attached removable disks then extorts the user for money to release the encryption key.234**

Ransomware.

1. **True or false? Most anti-virus software can remediate a system by blocking access to an infected file but not actually deleting it.**

True—this is called quarantining the file.

1. **What is the main means by which anti-virus software identifies infected files?**

Using definitions or signatures of known virus code. These definitions must be kept up-to-date.

1. **What are the two main ways that spam might expose recipients to hazardous content?**

Through malware-infected attachments and through links to malicious websites.

1. **Your friend sent you an email link, which you have opened, and now the browser is asking whether you should install a plug-in to view all the content on the page. Should you proceed?**

No—this is a classic phishing attack and your friend's computer could be infected with a virus or Trojan. Check whether they sent the link in good faith first.

1. **True or false? An OEM site is a reputable source of management software and drivers for a particular system.**

True—an Original Equipment Manufacturer (OEM) in the IT industry, such as Dell or HP, assembles systems made from the parts and software of various other suppliers. The components used in their systems may be specific to their brand and so they host their own support files for any system they sell.

# Module 5 / Unit 3 / Using Access Controls

1. **What are the four processes of an access control system?**

Identification, Authentication, Authorization, and Accounting.

1. **Users should only be granted the minimum sufficient permissions. What system policy ensures that users do not receive rights unless granted explicitly?**

Implicit deny.

1. **What is the main type of non-discretionary access control?**

Mandatory Access Control—though any rules-based system might restrict discretionary aspects of granting rights.

1. **What type of control prevents a user from denying they performed an action?**

Non-repudiation. Examples of controls providing non-repudiation include logging, video surveillance, biometrics, signatures, and receipts/tokens.

1. **What sort of account allows someone to access a computer without providing a user name or password?**

Guest account.

1. **How does a one-time password work?**

The password is generated by an asymmetric encryption algorithm. This means that the authenticating server can determine that the number was generated by a particular device (fob) at a particular time. When used with a PIN, it also proves that the password was input by a particular user.

1. **What type of system allows a user to authenticate once to access multiple services?**

Single Sign-On (SSO).

1. **What type of cryptographic operation(s) are non-reversible?**

Cryptographic hashing. You might also mention asymmetric encryption and public/private key pairs, where an operation performed with one key can only be reversed by the linked key and NOT by the key that performed the original operation.

1. **What class of data is a transport encryption protocol designed to protect?**

Data in transit (or data in motion).

1. **Why is it important not to use simple words or names as a password?**

Password-cracking software is configured with dictionaries of such names and phrases. Even if the password is encrypted, if it matches a term in the password-cracking dictionary it will be discovered in seconds.

# Module 5 / Unit 4 / Behavioural Security Concepts

1. **What is a SOP?**

Standard Operating Procedure.

1. **Apart from passwords and PII, what other type(s) of confidential information should be governed by classification and handling procedures?**

Company confidential information and customer information.

1. **Why might a company ban use of the corporate network and desktop software for personal communications?**

The company might be held responsible for inappropriate content posted by its employees. The issue of privacy is also complex and it is often better for both the company and the employee to use corporate systems for business communications only.

1. **What two main privacy issues arise from using a social networking site?**

Firstly, you need to control how far information you post to the site is distributed. You could make it private, accessible to close friends only, accessible to all your contacts, or accessible to anyone. Secondly, you need to know how the company processes, stores, and transfers or sells any data it collects about you, including information you post and your activity on the site.