

# 9. Security

## Cybersecurity

- the characteristics of different threats to computer systems, including:
  - malware
  - phishing
  - social engineering
  - brute force attacks
  - denial of service attacks
  - data interception and theft
  - SQL injection
- different ways of protecting against threats during system design, creation, testing and use, including:
  - penetration testing
  - network forensics
  - anti-malware software
  - firewalls
  - user access levels
  - passwords
  - double authentication
  - encryption.

3. A large comprehensive school has over 500 computers connected to their *Local Area Network (LAN)* with a connection to the Internet.

(b) All staff and pupils have a unique *username* and a *password* to access the network.

State **three** rules that should apply to users' passwords to reduce the possibility of someone guessing a password. [3]

Rule 1 .....

.....

.....

Rule 2 .....

.....

.....

Rule 3 .....

.....

.....

2015

3. A large comprehensive school has over 500 computers connected to their *Local Area Network (LAN)* with a connection to the Internet.

(c) All pupil and staff files are stored on servers located in a secure server room.

(i) Describe the *user access levels* pupils should be given for their own files. [1]

.....  
.....

(ii) Describe the *user access levels* that should be given for files a teacher wants pupils to view, such as a homework task. [1]

.....  
.....

2015

2017

Cyber security is essential in the protection against different types of malware.

(a) Describe **two** methods of protection against the use of key loggers. [4]

.....

.....

.....

.....

.....

.....

.....

.....

.....

(b) Describe **two** characteristics of a computer virus. [2]

.....

.....

.....

.....

2017

12. A large organisation stores confidential data about its customers on its network.

Describe the dangers that can arise from the use of networks and discuss the importance of network security, giving suitable security preventions for the organisation. [10]

.....

.....

.....

.....

.....


.....

.....

.....

.....

.....



Ms on next 2 slides

## Dangers

- Hacking - gain unauthorised access to data/to a computer system.
- Virus - a program which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
- Trojan - a program designed to breach the security of a computer system while ostensibly performing some innocuous function.
- Worm - a standalone malware computer program that replicates itself in order to spread to other computers.
- Spyware - software that enables a user to obtain information about another's computer activities by transmitting data from their hard drive.
- Botnets - a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.
- Malware - software which is specifically designed to disrupt or damage a computer system.
- Keylogger - a computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.
- Malicious damage - when a person intentionally sets out to corrupt or delete electronic files, data or software programs.
- Accidental damage - when a person unintentionally corrupts or deletes electronic files, data or software programs.

## Preventions

- Unique username and a strong secure password - the organisation limits access to the network by ensuring that all authorised users have unique username and a strong secure password.
- Access rights - access to confidential files on the network is limited to authorised users only by assigning access rights to users that only allow certain users to access specified area of the network and/or specified files.
- Encryption - hackers are prevented from reading the confidential files even they gain access to it by encrypting the files
- Encryption – an encryption key is used and known only by the organisation
- Firewall - the servers would be protected with firewall software blocking / checking all network traffic entering or leaving specified ports / stop programs accessing the internet
- Antivirus software - file servers would be protected with antivirus software which regularly scans all files stored on them for possible infection by malware
- Antivirus software - email server would be protected with antivirus software and all incoming emails would be scanned to see if attached files are infected
- Antivirus software - workstations would be protected with antivirus software and all files from external media would be scanned before they're allowed to be accessed
- Accounting or auditing software – all files accessed by a user are recorded in an activity log

Band	AO2 (Max 10 marks)
3	<p><b>8 - 10 marks</b></p> <p>The candidate has:</p> <ul style="list-style-type: none"> <li>• shown clear understanding of the requirements of the question and a clear knowledge of the indicative content. Clear knowledge is defined as a response that provides eight to ten relevant detailed points from the indicative content relating to both the dangers and the importance of network security with suitable security preventions, with a maximum of 5 marks for either aspect</li> <li>• addressed the question appropriately describing methods that the organisation can use to protect its data</li> <li>• produced writing which is very well structured using accurate grammar, punctuation and spelling</li> <li>• used appropriate technical terminology referring to the indicative content accurately</li> </ul>
2	<p><b>4 - 7 marks</b></p> <p>The candidate has:</p> <ul style="list-style-type: none"> <li>• shown adequate understanding of the requirements of the question and a satisfactory knowledge of the indicative content. Satisfactory knowledge is defined as a response that provides four to seven points from the indicative content relating to both the dangers and the importance of network security with suitable security preventions, with a maximum of 5 marks for either aspect</li> <li>• addressed the question describing methods that the organisation can use to protect its data</li> <li>• produced writing which is generally well structured using reasonably accurate grammar, punctuation and spelling</li> <li>• used appropriate technical terminology referring to the indicative content</li> </ul>

1	<p><b>1 - 3 marks</b></p> <p>The candidate has:</p> <ul style="list-style-type: none"> <li>• attempted to address the question but has demonstrated superficial knowledge of the indicative content. Superficial knowledge is defined as a response that provides one to three points from the indicative content relating to the dangers and/or the importance of network security with suitable security preventions</li> <li>• produced writing which shows some evidence of structure but with some errors in grammar, punctuation and spelling</li> <li>• used limited technical terminology referring to the indicative content</li> </ul>
0	<p><b>0 marks</b></p> <p>Response not credit worthy or not attempted.</p>



10. Internet protocols, operating systems and network equipment all present inherent technical vulnerabilities that must be identified and protected against.

(a) Describe the following forms of attack on cybersecurity:

(i) SQL injection. [2]

.....

.....

.....

.....

.....

(ii) IP address spoofing. [2]

.....

.....

.....

**2018**

*(b)* Describe methods of identifying these vulnerabilities.

**[8]**

.....

.....

.....

**Ms on next slide**

# 2018

## Footprinting.

- Footprinting is the first step in the evaluation of the security of any computer system.
- It involves gathering all available information about the computer system or network and the devices that are attached to it.
- Footprinting should enable a penetration tester to discover how much detail a potential attacker could find out about a system
- and allow an organisation to limit the technical information about its systems that is publicly available.

## Ethical hacking

- Ethical hacking is carried out with the permission of the system owner to cover all computer attack techniques.
- An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers.
- This information is then used by the system owner to improve system security.

## Penetration testing

- Penetration testing is a sub set of ethical hacking that deals with the process of testing a computer system, or network to find vulnerabilities that an attacker could exploit.
- The tests can be automated with software applications or they can be performed manually.

## Penetration test strategies include;

- Targeted testing, testing carried out by the organization's IT team and the penetration testing team working together.
- External testing, to find out if an outside attacker can get in and how far they can get in once they have gained access.
- Internal testing, to estimate how much damage a dissatisfied employee could cause.
- Blind testing, to simulate the actions and procedures of a real attacker by severely limiting the information given to the team performing the test.

	7 - 0 MARKS
3	<p>The candidate has:</p> <ul style="list-style-type: none"> <li>• shown clear understanding of the requirements of the question and a clear knowledge of the indicative content. Clear knowledge is defined as a response that provides seven to eight relevant detailed points from the indicative content</li> <li>• addressed the question appropriately discussing methods of identifying vulnerabilities.</li> <li>• used appropriate technical terminology referring to the indicative content accurately.</li> </ul>
2	<p style="text-align: center;"><b>3 - 6 marks</b></p> <p>The candidate has:</p> <ul style="list-style-type: none"> <li>• shown adequate understanding of the requirements of the question and a satisfactory knowledge of the indicative content. Satisfactory knowledge is defined as a response that provides three to six points from the indicative content.</li> <li>• addressed the question, discussing methods of identifying vulnerabilities.</li> <li>• used appropriate technical terminology referring to the indicative content.</li> </ul>
1	<p style="text-align: center;"><b>1 - 2 marks</b></p> <p>The candidate has:</p> <ul style="list-style-type: none"> <li>• attempted to address the question but has demonstrated superficial knowledge of the indicative content. Superficial knowledge is defined as a response that provides one to two points from the indicative content.</li> <li>• used limited technical terminology referring to the indicative content</li> </ul>
0	<p style="text-align: center;"><b>0 marks</b></p> <p>Response not credit worthy or not attempted.</p>