T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber security

Assignment 2

Mark scheme

v1.1: Specimen assessment materials
21 November 2023
603/6901/2

Internal reference: DSS-0013-04

NCFE

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment (OSA)

Cyber Security

Mark scheme

Assignment 2

Marking guidelines

General guidelines

You must apply the following marking guidelines to all marking undertaken throughout the marking period. This is to ensure fairness to all students, who must receive the same treatment. You must mark the first student in exactly the same way as you mark the last.

The mark scheme must be referred to throughout the marking period and applied consistently. Do not change your approach to marking once you have been standardised.

Reward students positively giving credit for what they have shown, rather than what they might have omitted.

Utilise the whole mark range and always award full marks when the response merits them.

Be prepared to award 0 marks if the student's response has no creditworthy material.

Do not credit irrelevant material that does not answer the question, no matter how impressive the response might be.

The marks awarded for each response should be clearly and legibly recorded.

If you are in any doubt about the application of the mark scheme, you must consult with your team leader or the chief examiner.

Guidelines for using extended response marking grids

Extended response marking grids have been designed to award a student's response holistically for the relevant task or question and should follow a best-fit approach. The grids are broken down into levels, with each level having an associated descriptor indicating the performance at that level. You should determine the level before determining the mark.

Depending on the amount of evidence that the task produces, the grids will either be a single, holistic grid that covers the range of relevant performance outcomes (POs), and will require you to make a judgement across all the evidence, or they will consist of multiple grids, that will be targeted at specific POs, and will require you to make a judgement across all the evidence in relation to that particular grid in each case, therefore making multiple judgements for a single task to arrive at a final set of marks. Where there are multiple grids for a particular task, it is important that you consider all the evidence against each of the grids, as although the grids will focus on particular POs, awardable evidence for each grid may come from across the range of evidence the student has produced for the task.

When determining a level, you should look at the overall quality of the response and reward students positively, rather than focussing on small omissions. If the response covers aspects at different levels, you should use a best-fit approach at this stage and use the available marks within the level to credit the response appropriately.

When determining a mark, your decision should be based on the quality of the response in relation to the descriptors. Standardisation materials, marked by the chief examiner, will help you with determining a mark. You will be able to use exemplar student responses to compare to live responses, to decide if it is the same, better or worse.

To support your judgement, the indicative content is structured in such a way that mirrors the order of the different points within the band descriptors. This will allow you to use the 2 in conjunction with each other by providing examples of the types of things to look for in the response, for each descriptor. In other words, the indicative content provides you with a starting point of possible examples and the bands express the range of options

available to you in terms of the quality of the response. You should apply the standards that have been set at relevant standardisation events in a consistent manner.

You are reminded that the indicative content provided under the marking grid is there as a guide, and therefore you must credit any other suitable responses a student may produce. It is not a requirement either that students must cover all of the indicative content to be awarded full marks.

Performance outcomes

This assessment requires students to:

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data

PO2: Propose remediation advice for a security risk assessment

PO3: Discover, evaluate and apply reliable sources of knowledge

Task 1: investigate and take corrective action

Band	Mark	Descriptor
4	35–42	An excellent report identifying a detailed understanding of the differences between cyber attacks and software program problems. The report explains clearly and in detail how and why the issues have occurred and the type of attack it could be. An excellent demonstration of the ability to investigate and analyse existing potential issues whilst recommending the most effective remedial action. A clear and detailed outline of remedial actions and how these would better protect the current system, including wide ranging future recommendations.
3	23–34	A good report identifying a mostly clear and detailed understanding of the differences between cyber attacks and software program problems. The report explains how and why the issues have occurred and the type of attack it could be in a mostly clear and detailed manner. A good demonstration of the ability to investigate and analyse existing potential issues whilst recommending effective remedial action. A good outline of remedial actions and how these would better protect the current system, including appropriate future recommendations.
2	11–22	A reasonable report identifying some understanding of the differences between cyber attacks and software program problems. The report explains satisfactorily how and why the issues have occurred and the type of attack it could be. A reasonable demonstration of the ability to investigate and analyse existing potential issues whilst recommending remedial action. A reasonable outline of remedial actions and how these would better protect the current system, including some future recommendations.
1	1–10	A basic report identifying a limited understanding of the differences between cyber attacks and software program problems. The report gives a limited explanation as to how and why the issues have occurred and the type of attack it could be. A limited demonstration of the ability to investigate and analyse existing potential issues whilst recommending remedial action. A limited outline of remedial actions and how these would better protect the current system, including limited future recommendations.
	0	No creditworthy material.

Indicative content

Part A

When explaining how to identify the difference between a cyber attack and an internal software program problem, there should be information relating to the fact that a cyber attack is the deliberate exploitation of a computer system and could affect the whole system and an internal software problem could be on a lot smaller scale for example, one device and the only real way to differentiate would be through an investigation.

To determine if it is a cyber attack or internal software problem at the root of issue the use of software will be required as detailed below. After the investigation is complete there will normally be enough evidence to make a judgement on the root of the problem.

Cyber attack

- malware/virus scans to identify infections in the system
- vulnerability scanning to verify vulnerabilities in the system, for example, open ports, running services not needed, poor system configurations and missing passwords
- network traffic analysers to view network activity that could identify rogue connections and IP addresses
- log file evidence to view system activity and see if there are any errors

Software

- apply software updates/patches
- uninstalling and reinstalling the software
- view task manager processes and information
- clean the registry
- check internal storage
- check network configuration if accessing online services and data

Types of attack

Although the attack is most likely malware based on the scenario other methods could be considered at this stage such as:

- drive-by download – malicious script inserted into web page
- phishing – a form of social engineering, although not directly mentioned in the scenario it could be a consideration
- brute-force attack – use of mathematical methods (for example, referring to a dictionary) to attempt to guess login in details in order to access the device and network
- man-in-the-middle attack – resulting from using unsecured Wi-Fi connections when logging into public internet connections
- cross-site scripting (XSS) – injection of malicious code into a web application, allowing access to a user's browser

Part B

Students should provide screenshots of the results of the scan.

The emails have issues relating to:

Email 01 – Invoice 24887024 from Lockman, Gorczany and Cole

This email has a link that does not work, but it also has an attachment named dawning wall up.zip.

This zip archive contains an .exe file which is malicious.

The exe file should be uploaded to the Virustotal website and the results returned will detail the infections found from various vendors that detail the infection as a trojan.

Information relating to the dangers of running executables that are email attachments and also running these types of file from unknown sources should be included.

Email 02 – Payment Notification

This email has an attachment named Bill Payment_000010818.xls.

The xls file should be uploaded to the Virustotal website and the results returned will detail the infections found from various vendors that detail the infection as a trojan.

Information relating to the dangers of macro viruses that can be hidden inside office files should be included.

Email 03 – About Your Card Membership!

This email has an attachment named AmericanExpress.html.

This HTML file is a fake login page for American Express. It is designed to steal someone's login credentials, and it is not malware that would infect a Windows computer.

Information relating to the dangers of filling out unsecure input forms and the unusual practice of distributing this in an email should be included.

The results provided by the assessment will highlight the issues that need addressing. The issues should be addressed by the student and evidenced with descriptions to demonstrate how the problem would be fixed.

Part C

Potential remedial action can include:

- cyber awareness training for staff to equip them with skills to identify malicious content
- real-time malware/virus scans to identify possible malicious content that could be downloaded
- email threat scanning
- firewall rules to block certain services/protocols and ports
- disable macros
- group policy rules to block executable downloads
- device hardening
- operating system (OS) hardening
- network monitoring
- auditing
- access controls

Note: The above list is not exhaustive, credit should be given to other suggestions as appropriate to the scenario in the brief

Task 2: ongoing maintenance

Band	Mark	Description
4	16–18	The student gives an excellent evaluation of the ongoing maintenance needed to ensure the system remains secure and operational in the future. There is an excellent justification of recommended remedial action alongside a thorough consideration of how these actions will be managed, whilst providing a detailed explanation of any upgrades as required.
3	11–15	The student gives a good evaluation of the ongoing maintenance needed to ensure the system remains secure and operational in the future. There is an appropriate justification of recommended remedial action alongside a mostly clear and detailed consideration of how these actions will be managed, whilst providing a clear explanation of any upgrades as required.
2	6–10	The student gives a reasonable evaluation of the ongoing maintenance needed to ensure the system remains secure and operational in the future. There is a satisfactory justification of recommended remedial action alongside a sound consideration of how these actions will be managed, whilst providing a satisfactory explanation of any upgrades as required.
1	1–5	The student gives a basic evaluation of the ongoing maintenance needed to ensure the system remains secure and operational in the future. There is a basic justification of recommended remedial action alongside a limited consideration of how these actions will be managed, whilst providing a basic explanation of any upgrades as required.
	0	No creditworthy material.

Indicative content

Maintenance and remedial activities

Information could include an evaluation of the following methods that demonstrates the type of maintenance activities that could take place:

- scheduled malware/virus scans
- scheduled vulnerability scanning, for example, Acunetix and Nessus
- scheduled network traffic analysis, for example, Wireshark
- analysis of log files, for example, SolarWinds
- scheduled software updates/patches, for example, Windows Server Update Services (WSUS)
- remote monitoring and management (RMM), for example, Microsoft Intune
- regular cyber awareness training, for example, iHasco

- introduction of biometrics on devices and premises
- multi factor authentication (Windows Server)

Learners should use a clear framework to structure their evaluation (for example, pros/cons, plus minus interesting (PMI) with an overall conclusion).

Note: The above list is not exhaustive, credit should be given to other suggestions as appropriate to the scenario in the brief

Performance outcome grid

Task	PO1	PO2	PO3	Total
1	24	18	0	42
2	0	0	18	18
Total marks	24	18	18	60
% weighting	40%	30%	30%	100%

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Post approval, updated for publication		01 June 2023
v1.1	Sample added as a watermark	November 2023	21 November 2023