CAMBRIDGE ADVANCED NATIONALS

CAMBRIDGE OCR

Sample assessment material

Cambridge Advanced National in

Cyber Security and Networks

Cambridge OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security

Extended Certificate | H137

F197: Penetration testing and incident response

Version 3.0

ocr.org.uk/cambridge-advanced-nationals

Introduction

This is sample assessment material (SAM). It is an example Cambridge OCR-set assignment that we publish alongside a new specification to help illustrate the intended style and tasks of our set assignments.

We also produce two further specific resources to support you with using this SAM:

- An assessment story where we explain the research we have undertaken during the development of the qualification and how consultation with teachers, students and schools has helped shape our assessment approach.
- A student guide to NEA assignments in which we provide a summary for your students of key points about their Cambridge OCR-set assignments, including the importance of avoiding plagiarism.

Summary of updates

Section	Change	Version	Date
General	New covering pages added.	3.0	June 2026
Throughout	Words highlighted (**could, must**) Typographical amends not affecting content		

CAMBRIDGE
OCR

Cambridge OCR-set Assignment

Sample Assessment Material

Cambridge OCR Level 3 Alternative Academic Qualification
Cambridge Advanced National in Cyber Security and Networks

Unit F197: Penetration testing and incident response

Scenario Title: Credit General Secure System

Valid for assessment until 20XX to 20XX.
For use by students beginning the qualification in September 20XX.

This is a sample Cambridge OCR-set assignment which should only be used for practice**.**

This assignment **must not** be used for live assessment of students.

The live assignments will be available on our secure website, 'Teach Cambridge'.

The Cambridge OCR administrative codes linked to this unit are:

- unit entry code F197
- certification code H137

The regulated qualification number linked to this unit is:

610/6208/X

Duration

About 15 hours of supervised time (GLH)
(work that **must** be completed under teacher supervised conditions)

Contents

Information and instructions for teachers

Using this assignment

This assignment provides a scenario and set of related tasks that reflect how organisations plan and complete penetration tests and how they respond to cyber security incidents.

You can give this to students on or after 1 June 202X to help them understand it before they start using it for assessment. The dates for which students can use it for assessment are shown on the front cover.

The assignment:

- Is written so that students have the opportunity to meet the requirements of all assessment criteria for the unit.
- Will tell students if their evidence must be in a specific format. If the task does not specify a format, students can choose the format to use.
- **Must** be completed under teacher supervision.

We have estimated that this assignment will take about 15 hours of supervised time to complete. Students should need approximately:

- 5 hours to complete Task 1.
- 3 hours to complete Task 2.
- 4 hours to complete Task 3.
- 3 hours to complete Task 4.

You **must**:

- Use a Cambridge OCR-set assignment for summative assessment of students.
- Familiarise yourself with the assessment criteria and assessment guidance for the tasks. These are given at the end of each student task. They are also with the unit content in **Section 5** of the Specification.
  Assessment guidance is only given where additional information is needed.
  There might not be assessment guidance for each criterion.
- Make sure students understand that the assessment criteria and assessment guidance tell them in detail what to do in each task.
- Read and understand **all** the rules and guidance in **Section 7** of the Specification **before** your students start the set assignments.
- Make sure that your students complete the tasks and that you assess the tasks fully in line with the rules and guidance in **Section 7** of the Specification.
- Give your students the **Cyber Security and Networks Student guide to NEA assignments before** they start the assignments.
- Complete the **Teacher Observation Record** for **Task 2**. You **must** follow the guidance given when completing it.

You **must not**:

- Use live Cambridge OCR-set assignments for practice or formative assessment. This sample assessment material **can** be used for practice or formative assessment.
- Use this sample assessment material for live assessment of students.
- Allow group work for **any** task in this assignment.
- Change any part of the Cambridge OCR-set assignments or assessment criteria.

Information for delivering tasks

Task	Requirements
Task 2	P7 requires students to demonstrate **three** exploitation activities which have been identified in P5 and included in their exploitation activities test plan in P6. The exploitation activities students demonstrate need to be carefully selected to make sure that the centre has resources for those chosen. This criterion does **not** have to be completed in the context of the scenario or using an IT system which has the same level of complexity as the organisation's system in the scenario. Students **could** demonstrate their ability to access and compromise IT systems using in-centre simulations, role play and browser-based cyber security training platforms. Examples of browser-based cyber security training platforms include: • https://tryhackme.com/ • https://www.hackthebox.com/.

Pages 1-4 are for teachers only. Please do **not** give **Pages 1-4** to your students.

You can give **any** or **all** of the pages **that follow** to your students.

Tasks for students and assessment criteria

Unit F197: Penetration testing and incident response

Scenario title: Credit General secure system

Valid for assessment from September 20XX to 20XX.
For use by students beginning the qualification in September 20XX.

Scenario

Credit General is a British based commercial bank. The business plans to expand their services into the British personal banking sector. Credit General aims to provide their personal banking customers with a flexible but secure means of access to their accounts.

Credit General has developed a web-based business model which comes with risks. They are aware of implications to their business operations if any of their customer data was compromised or their service disrupted. Credit General are preparing to launch a new personal banking service. You are part of Credit General's cyber security team. Credit General have asked you to investigate exploitation activities on their network, employees and cloud-based business to test for any security flaws.

Vulnerabilities can exist anywhere within the internal and external infrastructure so all aspects of the system will need to be investigated. Financial and customer data are common areas that threat actors are likely to take advantage of.

Credit General uses a key card system for employees to enter their buildings. This system is based on Radio Frequency Identification (RFID). The buildings use both wired and wireless network connectivity.

Credit General uses Office 365 with Two Factor Authentication (2FA) enabled. All data files are backed up online.

If they wish to, employees may work from home using their own IT equipment and internet connection. In-house apps are run from local servers and can be accessed by the user initiating a connection to the Remote Desktop Server. Access to in-house apps is password protected and based on user permissions.

You have set up a red team to attack and find areas of the system that could lead to data theft with a timescale of two weeks.

Following the red team being set up several unusual events have been reported.

- Employees at Credit General have received an email asking them to verify their account credentials. Some employees have reported the email as suspicious; however, some have reported that they handed over their credentials after they clicked the link in the email.

- After receiving technical support, employees have received a link to a survey asking them about their experiences of the support provided. When they clicked the link, employees reported it led to a blank webpage.

- An employee has reported that their work laptop was stolen from their car overnight. The laptop contained sensitive information.

- Credit General's IT support team have identified an increase in Domain Name System (DNS) traffic outside of standard business hours. When they investigated the system logs, they discovered that a large amount of data was sent from an IP address of an employee to external IP addresses.

Task 1

Creating a penetration testing scoping plan

Topic Areas 1, 2 and 6 are assessed in this task

The task is:

Create a penetration testing scoping plan for Credit General.

- Explore vulnerabilities and impacts of cyber security incidents for the organisation.
- Create a penetration testing scoping plan.

Your evidence **must** include:

- A penetration testing scoping plan.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P1: Use research to **explain** why the data stored on the IT system in the organisation system would be of interest to threat actors. (PO4)	**M1: Explain** the vulnerabilities of the IT system in the organisation. (PO2)	**D1: Assess** the potential impacts of cyber security incidents on the organisation. (PO3)
P2: Describe the planning considerations needed to create the penetration testing scoping plan. (PO2)	**M2: Justify** which vulnerabilities of the IT system in the organisation the penetration plan will focus on. (PO3)	**D2: Justify** the choices of the penetration testing strategies included in the penetration testing scoping plan. (PO3)
P3: Describe the information requirements needed for each planning consideration for the penetration testing scoping plan. (PO2)		
P4: Create the penetration testing scoping plan for the IT system in the organisation. (PO4)	**M3: Explain** the role that the team(s) would play in the planned penetration testing. (PO2)	

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P1	• Students **could** research IT systems like the one in the scenario to gain insight into the types of data stored. Students **must** explain why each type of data identified would be of interest to threat actors and the benefits to a threat actor of accessing/stealing it.
P2	• Students **must** contextualise the planning considerations in Topic Area 2.3, so they relate to the IT system in the scenario.
P3	• This is the information required by students to create their penetration testing scoping plan in P4. Topic area 2.3 includes a list of penetration testing planning considerations.
P4	• Students **must** include the components of penetration testing scoping plans listed in Topic Area 2.3 when creating their penetration testing scoping plan.
M1	• Students **must** explain why each vulnerability listed in Topic Area 1.3 is a potential issue for the organisation in the scenario.
M2	• Students **must** justify which vulnerabilities in the IT system they have included in their penetration testing scoping plan and why.
M3	• Students **must** explain the role that the team(s) play in the context of the scenario. The explanation **must** include the actual tasks the team(s) would be doing in the planned penetration testing rather than a generic description of what a team's role is.
D1	• There is no assessment guidance for this criterion.
D2	• Students **must** justify the choices of penetration testing strategies included in their penetration testing scoping plan. Penetration testing strategies which are not included in Topic Area 2.1 **could** also be included.

Advice:

- Remember to clearly reference any information used from books, websites, or other sources to support your evidence.

Task 2
Planning exploitation activities

Topic Areas 1, 2, 3 and 6 are assessed in this task

The task is:

Create the exploitation activities test plan for Credit General.

- Identify exploitation activities that could be used to target the IT system in the organisation.
- Create the exploitation activities test plan.
- Demonstrate exploitation activities.

Your evidence **must** include:

- An exploitation activity test plan
- Written evidence.
- A Teacher Observation Record (TOR) form signed by you and your teacher.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P5: Identify the activities to be included in the exploitation activities test plan for the IT system in the organisation. (PO2)	**M4: Explain** the suitability of the planned exploitation activities to test the vulnerabilities of the IT system in the organisation. (PO2)	**D3: Discuss** the likelihood of the planned exploitation activities being conducted by threat actors. (PO3)
P6: Create the exploitation activities test plan for the IT system in the organisation. (PO4)		
P7: Demonstrate three exploitation activities from the exploitation activities test plan. (PO4)		

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P5	• Students **must** identify all the exploitation activities that need to be planned so the IT system in the scenario is tested for vulnerabilities. This criterion **could** be evidenced separately or as part of the exploitation activities test plan created in P6.
P6	• Students **must** create an exploitation activities test plan to test the IT system in the scenario for vulnerabilities. The structure of the exploitation activities test plan is in Topic Area 2.4.
P7	• Students **must** demonstrate **three** exploitation activities from their exploitation activities test plan created in P6, which centres have resources for. This criterion does not have to be completed in the context of the scenario or using an IT system which has the same level of complexity as the organisation's system in the scenario. • A Teacher Observation Record (TOR) form **must** be provided for each student as evidence of demonstrating exploitation activities. Students **must** read and sign the TOR form. The TOR form **must** provide clear evidence that the student has demonstrated **three** exploitation activities from their exploitation activities test plan created in P6. The TOR form **must** include a description of how each exploitation activity was completed by the student including the tools and techniques they used, and the success of the exploitation activity. For other criterions in this task the student must provide suitable evidence in the form of an exploitation activity test plan and written evidence.
M4	• Students **must** take the identified exploitation activities from P5 and look at the suitability of each in identifying and taking advantage of vulnerabilities.
D3	• Students **must** discuss the likelihood of each planned exploitation activity actually happening. Students do not need to specify the type of a threat actor who could conduct the exploitation.

Task 3
Planning a response to cyber security incidents

Topic Areas 1, 4 and 6 are assessed in this task

The task is:

Create a cyber security incident response plan for Credit General.

- Create a cyber security incident response plan.
- Explain the management of the cyber security incident.
- Create an incident response playbook.

Your evidence **must** include:

- A cyber security incident response plan.
- An incident response playbook for an exploitation activity.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P8: Create a cyber security incident response plan which shows how the organisation should respond to **one** cyber security incident. (PO4)	**M5: Explain** the suitability of the cyber security incident response plan in containing the incident. (PO2)	**D4: Evaluate** the strengths and weaknesses of your approach taken when responding to and managing cyber security incidents. (PO3)
P9: Explain how the organisation should manage the cyber security incident in **P8**. (PO2)		
P10: Create an incident playbook for **one** cyber security incident. (PO4)	**M6: Explain** the suitability of the incident playbook in preventing the success of the cyber security incident. (PO2)	

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P8	• Students **must** produce a cyber security incident response (CSIR) plan for **one** incident identified in the scenario **or one** from their exploitation activities test plan. The structure of the CSIR plan is in Topic Area 4.1.
P9	• The explanation **must** be for the cyber security incident the student chooses for P8. If students do not achieve P8, it is still possible to achieve this criterion. • Students **must** include in their explanation each of the incident management stages in Topic Area 4.2.
P10	• Students **could** base their incident playbook on the incident from P8, a different incident from the scenario or one they have identified. The content requirements of the incident playbook are in Topic Area 4.3.
M5	• M5 builds on P8. Students **must** explain the suitability of the plan for containing the incident chosen in P8.
M6	• M6 builds on P10. Students **must** explain the suitability of the playbook in preventing the success of the incident chosen in P10.
D4	• There is no assessment guidance for this criterion.

Task 4
Creating a maintenance plan

Topic Areas 1, 5 and 6 are assessed in this task

The task is:

Create a maintenance plan to build and upkeep incident response capability for Credit General.

- Create a maintenance plan.
- Create training materials for exploitation activities.

Your evidence **must** include:

- A maintenance plan.
- Training materials.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P11: Create a maintenance plan to build and upkeep cyber security incident response capability for the organisation. (PO4)	**M7: Explain** how the maintenance plan would improve the organisation's cyber security. (PO2)	**D5: Discuss** the strengths and weaknesses of the organisation's cyber security provision. (PO3)
P12: Create training materials for **two** different types of exploitation activity from the exploitation activities test plan. (PO4)		

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P11	• Students **must** create a maintenance plan for the organisation in the scenario. The content of a maintenance plan is in Topic Area 5.1.
P12	• Students **must** create training materials for **two different** types of exploitation activities included in their exploitation activities test plan created in **Task 2**. If students do not achieve P6, it is still possible to achieve this criterion. • Examples of training materials which **could** be created are in Topic Area 5.2. However, this list is not definitive, and students **could** create any suitable training materials.
M7	• Students **must** include in their explanations why the maintenance will help the organisation in the scenario to be less likely affected by cyber security incidents and exploitations in the future.
D5	• Students **must** discuss the strengths and weaknesses of the organisation's cyber security provision after their cyber security incident response (CSIR) plan, playbook, maintenance plan and training materials created and used.

Teacher Observation Record Form

Use this form to record what is observed.
Read the **guidance notes** below the form **before** you complete the form.

Cambridge OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate)

Unit number:	F197
Unit title:	Penetration testing and incident response
Task number:	2
Task title:	Planning exploitation activities

Student's name:	
Date the activity was completed:	

What extra evidence is attached to the form?	

The **teacher** fills in this section:

What Assessment Criteria does this activity relate to? **P7:** Demonstrate three exploitation activities from the exploitation activities test plan.
How does the activity meet the requirements of the Assessment Criteria? You **must** describe: 1. What the student did 2. How it relates to the Assessment Criteria

Teacher's name:	
Teacher's signature:	
Date:	

The **student** fills in this section:

I agree with my teacher's description of how I completed this activity	Yes ☐
Use this space to make any extra comments.	
Student's signature:	
Date:	

Guidance notes

Both the teacher **and** the student are responsible for completing this form.

The **teacher must**:
- use the form to describe in detail what they observed the student doing.
- give contextualised details of what the student did and how this relates to the Assessment Criteria.
- say how well the activity was completed in relation to the Assessment Criteria with reasons.
- share what they have written with the student and offer the opportunity to discuss if the student disagrees with what is written.
- reach agreement with the student before the work is submitted for moderation.
- sign and date the form as evidence of agreement.

The **student must**:
- reach agreement with the teacher before the work is submitted for moderation.
- use the form to show that they agree with the teacher's record of the activity observed.
- sign and date the form as evidence of agreement.

The form **must**:
- be accompanied by extra evidence, as required by the task.
- provide evidence that is individual to the student.

The form **must not**:
- contain a simple repeat of the Assessment Criteria.
- contain just a list of skills.
- be completed by anyone other than the teacher observing the activity and the student completing the activity.
- be written by the student for the teacher to sign.
- be used to evidence achievement of a whole unit or task in isolation.

NEA Command Words

The table below shows the command words that may be used in the NEA assignments and/or assessment criteria.

Command Word	Meaning
Adapt	• Change to make suitable for a new use or purpose
Analyse	• Separate or break down information into parts and identify their characteristics or elements • Explain the different elements of a topic or argument and make reasoned comments • Explain the impacts of actions using a logical chain of reasoning
Assess	• Offer a reasoned judgement of the standard or quality of situations or skills. The reasoned judgement is informed by relevant facts
Calculate	• Work out the numerical value. Show your working unless otherwise stated
Classify	• Arrange in categories according to shared qualities or characteristics
Compare	• Give an account of the similarities and differences between two or more items, situations or actions
Conclude	• Judge or decide something
Describe	• Give an account that includes the relevant characteristics, qualities or events
Discuss (how/whether/etc)	• Present, analyse and evaluate relevant points (for example, for/against an argument) to make a reasoned judgement
Evaluate	• Make a reasoned qualitative judgement considering different factors and using available knowledge/experience
Examine	• To look at, inspect, or scrutinise carefully, or in detail
Explain	• Give reasons for and/or causes of something • Make something clear by describing and/or giving information
Interpret	• Translate information into recognisable form • Convey one's understanding to others, e.g. in a performance
Investigate	• Inquire into (a situation or problem)
Justify	• Give valid reasons for offering an opinion or reaching a conclusion
Research	• Do detailed study in order to discover (new) information or reach a (new) understanding
Summarise	• Express the most important facts or ideas about something in a short and clear form

We might also use other command words but these will be:

- commonly used words whose meaning will be made clear from the context in which they are used.
- subject specific words drawn from the unit content.

Tell us what you think

Your feedback plays an important role in how we develop, market, support and resource qualifications now and into the future. We want you and your students to enjoy and get the best out of our qualifications and resources, but to do that we need your honest opinions to tell us whether we're on the right track or not.

You can email your thoughts to support@ocr.org.uk or visit our feedback page to learn more about how you can help us improve our qualifications.

Designing and testing in collaboration with teachers and students

Helping young people develop an ethical view of the world

Equality, diversity, inclusion and belonging (EDIB) are part of everything we do

---

Contact the team at:

01223 553998

ocr.org.uk

To stay up to date with all the relevant news about our qualifications, register for email updates at ocr.org.uk/updates

Visit our Online Support Centre at support.ocr.org.uk

Sign up for Teach Cambridge to access your planning, teaching and assessment support material.

CAMBRIDGE
UNIVERSITY PRESS & ASSESSMENT