Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 7 January 2019 – Friday 25 January 2019

Supervised hours: 4 hours	Paper Reference **20158K**

Information Technology

Unit 11: Cyber Security and Incident Management

Part B

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this paper is 37.

Turn over ▶

Pearson

Instructions to Teachers/Tutors and/or Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments* (ICEA) document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *Instructions for Conducting External Assessments* (ICEA) document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of three weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for candidate use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Teachers/tutors may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Teachers/tutors and invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner’s work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

Each learner will need to submit 2 PDF documents, within their folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 29 January 2019.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your teacher/tutor may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents, within your folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your teacher/tutor.

Set Task Brief

Critically Endangered

Peter Russof is a computer programmer specialising in developing games for PCs. He has written several stand-alone games and has built up a profitable business as an independent game producer. Peter lives in Watford and works from home.

He has developed Critically Endangered (CE), a multiplayer online game set in a post-apocalyptic world. In CE a plague has caused man to be critically in danger of extinction. Peter's innovative idea was to use real world data such as maps, weather statistics, ecological and geographical information to create play areas. Players select a location in the real world and Peter's algorithms create a 3D play area of that location after the plague. Each player then creates, customises and controls their own player character, using it to interact with the play area and other players.

CE has an enthusiastic following of several thousand players with an active online community. Several of the players help by running a game forum and acting as guides and troubleshooters within the game environment.

Peter has gone into partnership with his cousin, Elana, who has run Romwebhost, a Romanian web hosting company, since 1998. Peter develops and supports CE while Elana supplies processing and hosting facilities through Romwebhost.

People who wish to play CE must create a user account and then log in via that account in order to access a play area.

Client brief

You advised Peter and Elana on security matters. Now, a few months later, Elana has called you in to review the investigation of a cyber security incident.

In December 2018 Elana received an email from an irate customer, complaining that his CE account had been hacked. Elana investigated the complaint because the customer had sent the email to her personal mailbox rather than the usual Support@CriticallyEndangered.com

Alex, the Cyber Security Manager at Romwebhost, told Elana that there had been an unusually high number of reports of compromised accounts in November 2018. Staff had dealt with the problem in accordance with the Incident Management Policy and Alex had not thought the incident serious enough to escalate further.

As there was a threat of possible legal action in the email, Elana asked Alex to investigate further. The matter was then discussed at a meeting.

Evidence items from the security incident at Romwebhost

Evidence items include:

1) Cyber Security Manager's report
2) Customer email
3) Notes from meeting to discuss the incident
4) Account security flowchart
5) Cyber security document – Incident Management Policy.

1 Cyber Security Manager's report

Compromised accounts, November 2018

Compromise categories
There was a higher than normal number of compromised accounts in November. These fell into three categories:

(a) Account lockouts due to incorrect password attempts. There were 296 instances logged, which is within normal expectations.

(b) Players reporting account penetration with damage to their player character. There were 105 instances. This figure is about 10 times greater than normal expectations. In every instance the damage followed a similar pattern. The player's character was used to create a message and then the character was put in a situation where it died. The message took several different forms, e.g. marked on a wall, scraped on the ground, but was always the same single word, 'Extinct'.

(c) Players reporting account penetration with effects other than category (b). There were 9 instances. This is within normal expectations. Reported effects varied but were all minor vandalism such as changing the player's name to something derogatory.

Compromise handling methods
Category (a) automatically by password recovery / security question system.
Category (b) manually by Support staff.
Category (c) manually by players, reversing the vandalism, with assistance from Support where needed.

Actions taken for category (b) compromises
Most reports came via in-game chat, others were emailed to Support.

- The first-line technician logged the incidents.
- The technician was able to restore player characters by using our back-up system.
- The technician received help from the in-game troubleshooters.
- The troubleshooters went into the affected play area to remove any traces of the attack, e.g. remove 'Extinct' and restore any damage caused by writing the word.
- Finally, a password change was enforced for the affected account.

Escalation of the problem
The technician dealt with several similar cases and followed procedures by escalating the problem to the Duty Manager. The Duty Manager recognised that this was a potentially serious threat and passed it on to the Cyber Security Team.

Actions taken by the Cyber Security Team
As the damage was easy to reverse, the Cyber Security Team decided to monitor the situation before taking any drastic action.

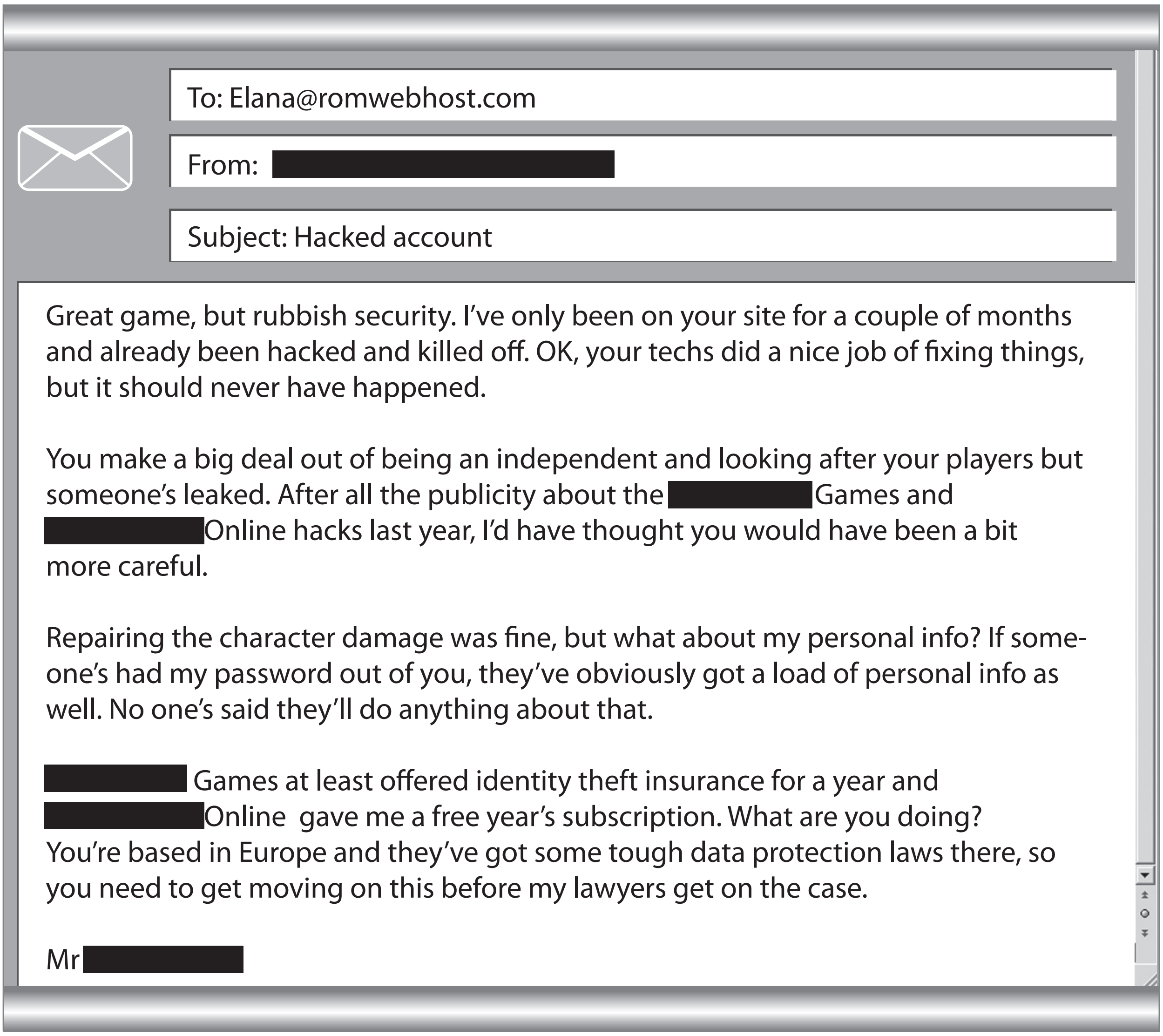
After a few more days, the Cyber Security Manager noted that:

- the number of compromises per day was increasing
- no way had been found of predicting which accounts would be compromised
- accounts that had been compromised and had their password changed had not been affected again.

He therefore decided to enforce a password change for all players except those already affected. The change was explained to players as being a routine security precaution.

No further category (b) compromises were reported and the incident was closed.

2 **Customer email (identifying information removed)**



To: Elana@romwebhost.com

From: [redacted]

Subject: Hacked account

Great game, but rubbish security. I've only been on your site for a couple of months and already been hacked and killed off. OK, your techs did a nice job of fixing things, but it should never have happened.

You make a big deal out of being an independent and looking after your players but someone's leaked. After all the publicity about the [redacted] Games and [redacted] Online hacks last year, I'd have thought you would have been a bit more careful.

Repairing the character damage was fine, but what about my personal info? If someone's had my password out of you, they've obviously got a load of personal info as well. No one's said they'll do anything about that.

[redacted] Games at least offered identity theft insurance for a year and [redacted] Online gave me a free year's subscription. What are you doing? You're based in Europe and they've got some tough data protection laws there, so you need to get moving on this before my lawyers get on the case.

Mr [redacted]

3 Notes from the meeting to discuss the incident

Those present; Peter, Elana, Alex, Maria (Romwebhost Legal Department)

Elana: Called meeting to order, asked Maria for legal opinion.

Maria: Mr [redacted] lives in New York, we have no physical presence in the USA, so a lawsuit is unlikely. Seems probable he is looking for a small payout in line with [redacted]Games and [redacted]Online.

Data protection penalties only apply if passwords were obtained from us, but an investigation would be expensive.

Legal Department needs to know if:

- passwords could have been stolen, by staff or external agent
- our security methods took into account what happened at [redacted]Games and [redacted]Online.

Alex: We wanted to get CE off to a good start, so had a separate physical server to the Romwebhost hosting business. We only used a few, experienced staff as technicians for CE. Theft by staff has a low probability. The security measures for player accounts were ported from Peter's previous version of the game.

Peter: I was aware of the [redacted]Games and [redacted]Online hacks, and several previous ones. I designed the system to be secure and not vulnerable to those hacks. **(Account security flowchart, evidence item 4, handed out.)**

In the [redacted]Games hack they stored passwords as plain text and relied on the database being secure. Someone did some database maintenance and left it linked to the internet. The hacker downloaded everything. The data went on sale for anyone to buy. We only store hashes.

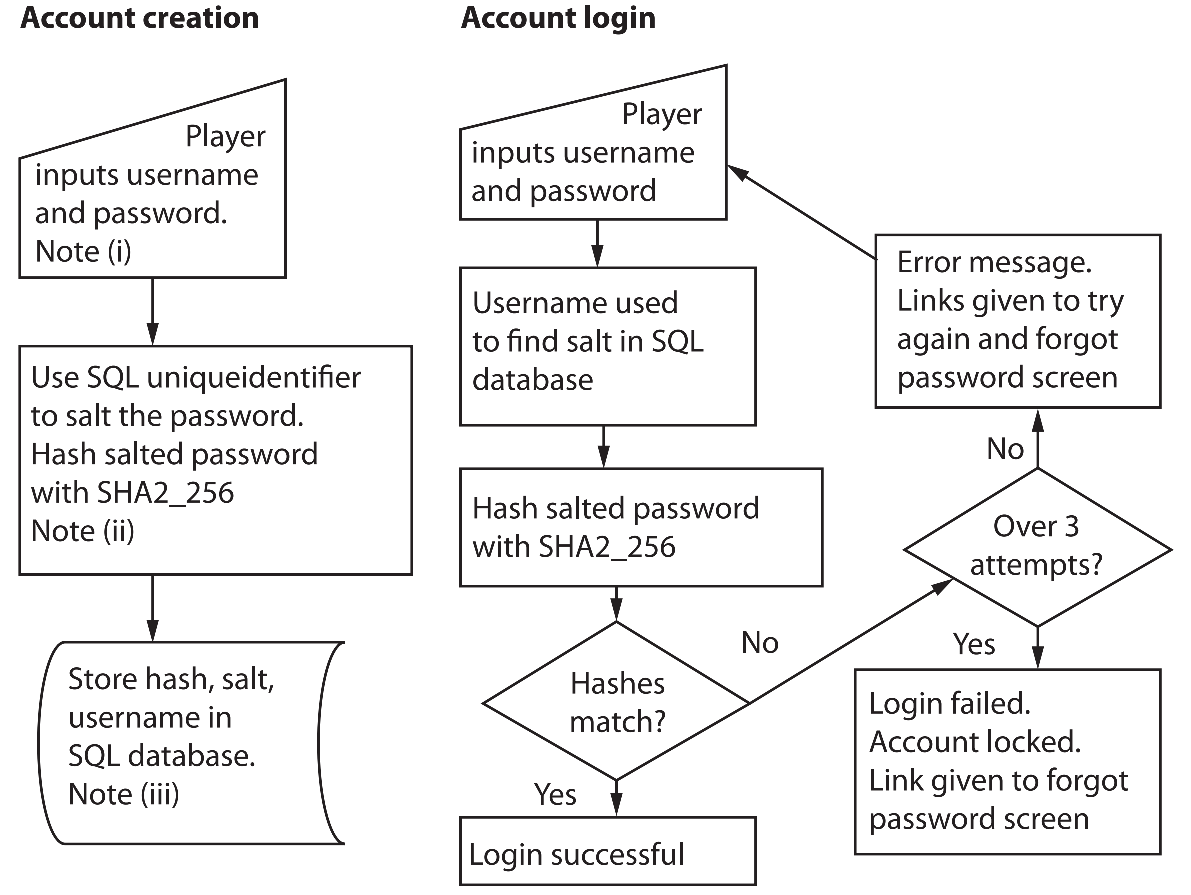
In the [redacted]Online hack I've heard that it was an SQL injection attack, we filter all our inputs so are protected there. [redacted]Online encrypted passwords and stored hashes like us, but only used the MD5 hashing algorithm. I moved the CE system to SHA2 some years ago. A sample of the [redacted]Online hashes was circulated, but then everything went quiet. Rumour says that [redacted]Online paid a ransom.

Alex: We checked the SQL filters and server security after the attack and everything was still in place. For obvious reasons, I don't think it was a brute force attack.

Elana: Summing up, we think we're still secure and are not legally liable. Just to be safe, we should ask someone from outside the company to review the incident.

Others: Agree.

4 Account security flowchart


Account creation
Player inputs username and password. Note (i)
Use SQL uniqueidentifier to salt the password. Hash salted password with SHA2_256 Note (ii)
Store hash, salt, username in SQL database. Note (iii)
Account login
Player inputs username and password
Username used to find salt in SQL database
Hash salted password with SHA2_256
Hashes match?
Yes
Login successful
No
Over 3 attempts?
No
Error message. Links given to try again and forgot password screen
Yes
Login failed. Account locked. Link given to forgot password screen

Notes.

i. Username is pre-populated from player's email address. This can be changed but most player's don't do that. Password must be a minimum of 8 characters.

ii. SQL uniqueidentifier is a 16 byte string generated by the computer on which the SQL database is running. It is globally unique (cannot be generated as uniqueidentifier by any other computer in the world). Using a salt prevents lookup table attacks.

iii. Only the hash, salt and username are stored. The password is discarded.

5 Cyber Security Documentation - Incident Management Policy

Incident management team

The Computer Security Incident Response Team (CSIRT) will be formed from the Cyber Security Team at Romwebhost.

The CSIRT will include:

- the first-line technician on duty at the time of the incident
- the Cyber Security Manager
- members of the Cyber Security Team nominated by the Cyber Security Manager.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to their line manager.
The manager will assess the threat and escalate it to the CSIRT leader if they consider it to be serious.
Initially it may be reported verbally but this must be followed up by an email. It is the responsibility of the CSIRT to maintain detailed documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of company data
- unauthorised access to company IT systems
- infection of company IT systems with malware.

Incident response procedures

(a) Theft of IT equipment

- Theft of IT equipment is a very serious issue. Any thefts must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen, etc.).
- The CSIRT team leader must ascertain if the item has actually been stolen (or if it is just missing).
- If the item is confirmed as stolen, CSIRT team leader must inform the police and contact the finance department so they can inform insurers.
- The CSIRT must prepare a report on the theft to Romwebhost senior management and if needed justify the finances required to replace the stolen item.

(b) Theft of company data

- Theft or loss of company data equipment may occur in a number of different ways.
- Any loss of company data must be reported at once to CSIRT team leader, initially a verbal report must be made followed up by email.
- The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.
- Having identified what has been lost or stolen and when, the CSIRT must retrieve backups and restore the data as soon as possible.
- The CSIRT should review the incident and implement procedures to prevent future losses.

(c) Infection of company IT systems with malware

Any member of staff who suspects that any IT system has been infected with malware must:

- Report at once to the CSIRT team leader, initially a verbal report must be made followed up by email.
- The infected system should be shut down as soon as possible.
- The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.

(d) Unauthorised access to company systems

- Any member of staff who suspects that there has been unauthorised access to any Romwebhost IT system must report it at once to their line manager.
- The manager will assess the situation and, if unauthorised access is confirmed, escalate the report to the CSIRT team leader, providing as much detail as possible (which system, how access was obtained). Initially a verbal report must be made, followed up by email.
- The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.
- The CSIRT will take whatever action is required to prevent future occurrences.
  A report must be sent to Romwebhost senior management.

Part B Set Task

You must complete ALL activities in the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You advised Peter and Elana on security matters. Now, a few months later, Elana has called you in to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at Romwebhost.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–4 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–5 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN TASK B = 3 MARKS
TOTAL FOR PAPER = 37 MARKS