T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

Assignment 2 – Pass

Guide standard exemplification materials (GSEMs)

v1.0: Specimen assessment materials
31 August 2023
603/6901/2

Internal reference: DSS-GSEM-18

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

Cyber Security

Guide standard exemplification materials (GSEMs)

Assignment 2 – Pass

Contents

Contents **2**

Introduction **3**

Assignment 2 ..... **4**

Task 1: investigate and take corrective action 4

Task 2: ongoing maintenance 14

Examiner commentary **18**

Overall grade descriptors 19

Document information **21**

Change History Record 21

Introduction

The material within this document relates to the Cyber Security occupational specialism sample assessment. These exemplification materials are designed to give providers and students an indication of what would be expected for the lowest level of attainment required to achieve a pass or distinction grade.

The examiner commentary is provided to detail the judgements examiners will undertake when examining the student work. This is not intended to replace the information within the qualification specification and providers must refer to this for the content.

After each live assessment series, authentic student evidence will be published with examiner commentary across the range of achievement.

Assignment 2

Task 1: investigate and take corrective action

Time limit

7 hours 30 minutes

You can use the time how you want, but all parts of the task must be completed within the time limit.

Brief

Tony has logged off the main system and has given you his laptop to work with. He has described the problems he has experienced when using his laptop as follows:

- applications are running slower than they used to
- programs are regularly freezing and not responding
- occasionally files are not opening

Firstly, you will be required to research what may be causing these issues.

You will then need to investigate and assess any vulnerabilities that may exist by analysing the emails and identifying any issues and possible resolutions.

Finally, you will be required to identify actions that could be taken to resolve the issues.

(42 marks)

Instructions for students

Part A

In relation to this brief, firstly you must create a report to:

- discuss how these issues could be the result of either a cyber attack or an internal software program problem – you should clearly identify how you would differentiate between the two
- explain how and why the issues could have occurred
- identify the type of attack it could be

Part B

You have full administration rights and access to Tony's laptop (this will be a virtual machine assigned to you by your tutor).

Using the virtual machine (VM) you have been assigned you must:

- log into the machine using the following credentials:
  - **username**: analyst
  - **password**: cyberops
- investigate the emails and assess any potential issues that may exist
- run a scan using the online tool **VirusTotal** to identify what attack, if any, has taken place

In your report you should:

- record your findings (this should include screenshots to evidence your investigation and use of the scan)
- suggest potential fixes for any issues that are identified

Part C

In your report you should:

- provide an outline of any remedial actions that could be implemented to better protect the current system (for example, any additional security methods that could be used), including any future recommendations

Evidence required for submission to NCFE

Report document including evidence from parts A, B and C

Student evidence

Part A

Background

Tony is a remote worker who logs into public and private internet when using his laptop.

He is concerned as he is experiencing the following issues with his laptop:

- slow running
- programs not responding
- files not opening

Malware versus application issues

Application Issues

Application issues cause applications to freeze and/or exit with an application error. There are many possible reasons for this as detailed below;

- if an application uses up too many resources, it may become unresponsive or crash - this can be caused by running too many applications simultaneously
- errors in the software can cause the application to freeze or crash - these errors can be caused for several reasons, such as incompatibility, obsolete software versions and unpatched software
- issues with the operating system or certain systems components (hardware and software) can cause applications to freeze or crash, for example outdated drivers
- hardware problems such as a device failure, caused by overheating for example
- issues with the network or internet connectivity can cause problems - these issues can be caused by poor connectivity, firewalls, or problems with the network infrastructure

Cyber Issues

Cyber attacks generally attempt to be covert so do not want anything they do to be recorded in logs or the end user to know. This is normally achieved through malware although there are other cyber attacks that are not convert such as Denial of Service (DOS). I will cover some of the main cyber attacks that Tony could be experiencing.

A cyber attack can infect an application with malware, which can cause the application to freeze or crash, it can modify an application's code or data, causing it to behave unexpectedly or become unstable. Malware can take many forms including spyware, viruses, trojans and worms. Tony could have unwittingly got infected with malware through one of the previously mentioned methods

A DoS attack involves flooding an application with traffic or requests, overwhelming its capacity to respond to legitimate requests. This can cause the application to become unresponsive or crash, resulting in application errors. This does seem unlikely for the problems Tony is encountering but without analysis of the system it cannot be ruled out.

Cyber attacks can exploit vulnerabilities in an application's code or network to cause it to become unstable. This can happen if an attacker finds and exploits a weakness in an application's security to execute malicious code or data, this can be caused by out of date or obsolete software.

Ransomware can cause an applications to freeze or crash by encrypting data on the computer or network. This can result in application errors or crashes if the application is unable to access the encrypted data. Like the DoS attack this seems an unlikely reason why Tony is experiencing his problem.

Social engineering attacks involve individuals divulging sensitive information or performing certain actions that can compromise the security of a computer or network. This can lead to the installation of malware or the exploitation of vulnerabilities, causing applications to freeze or crash, this can happen through email, webpages, SMS and telephone calls. Tony could well have done something unknowingly to divulge information that has had an effect on his system.

Analysis

To determine if it is a cyber attack or an internal software problem at the root of the issue, the use of software will be required. After an investigation has been undertaken there will normally be enough evidence to make a judgement on the root of the problem.

Below I have categorised the methods that could be used to determine if it is a cyber attack or an internal software program problem.

Cyber attack

Running malware/virus scans will help to identify any infections in the system. It is important that all malware/virus software is updated regularly so that the latest infections can be found. Using a network traffic analyser such as packet tracer can also be beneficial in determining if there is a cyber breach on Tony's device.

Internal software problem

Checking to see if the latest operating system and application software updates and patches have been applied. Windows update is a good source of this information and can inform the user of the last time the system was updated. Checking Windows event viewer and running utility software can also help with internal software problems.

Conclusion on the types of attack

The issues Tony is experiencing lead to a conclusion that there is a malware infection from a virus, Trojan or worm. These types of infections are normally associated with applications running slower than they used to, programs regularly freezing and not responding, and files not opening.

Part B

Investigation and analysis

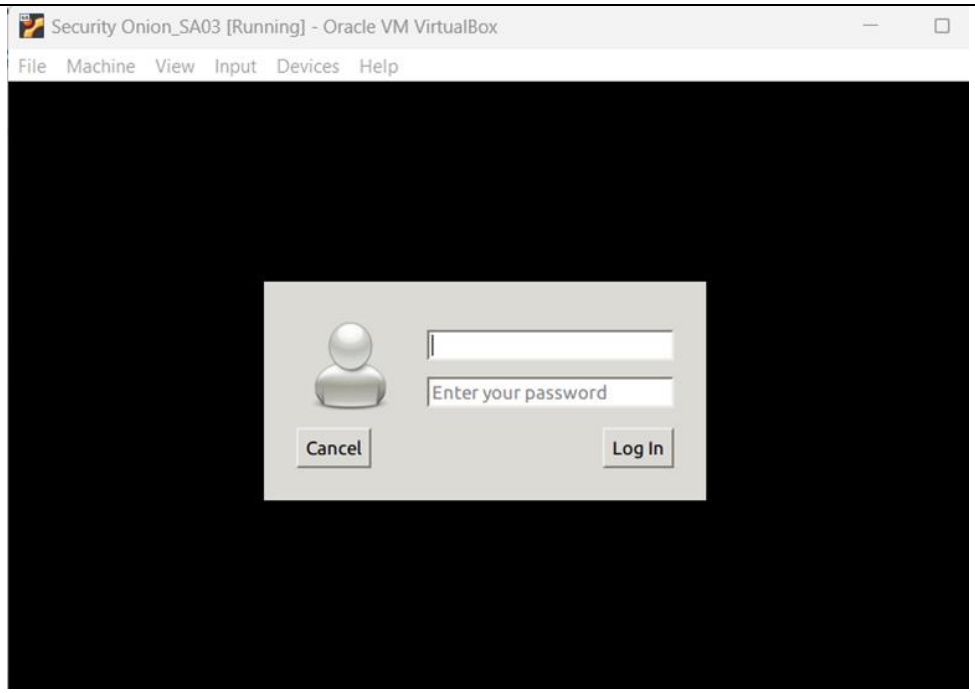
Tony is visiting the office so he has given me his laptop to see if I can determine the cause of the issues.

To investigate the cause of the problems I will be doing the following:

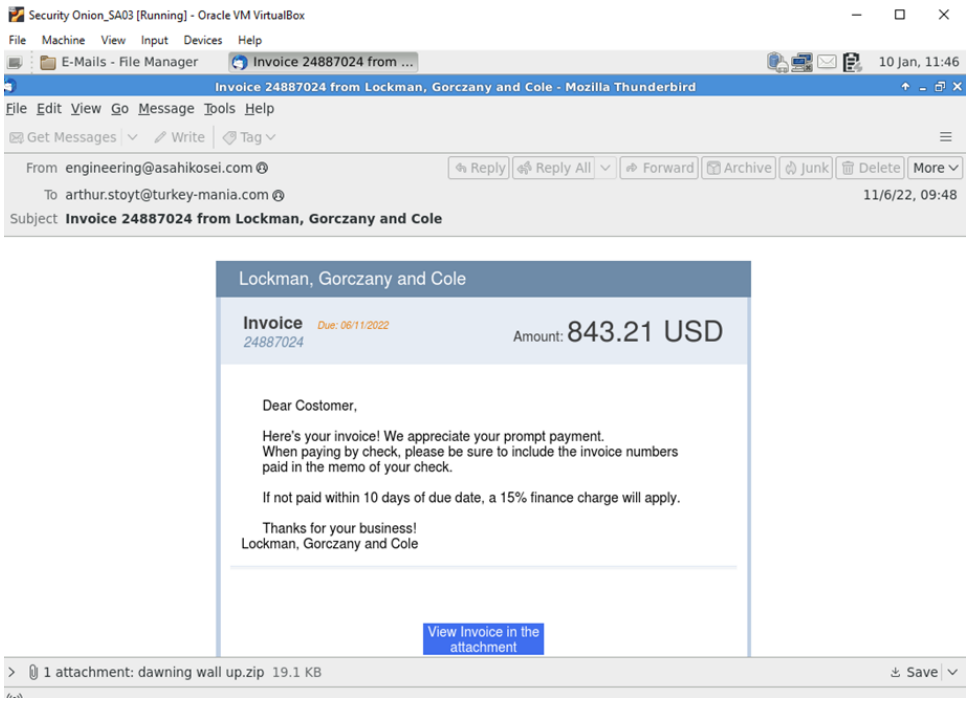
- log in to the machine provided using the supplied credentials
- analysing the emails to identify any potential issues
- use the virustotal.com website to see if the email attachments contain any potential malware/viruses

Machine investigation

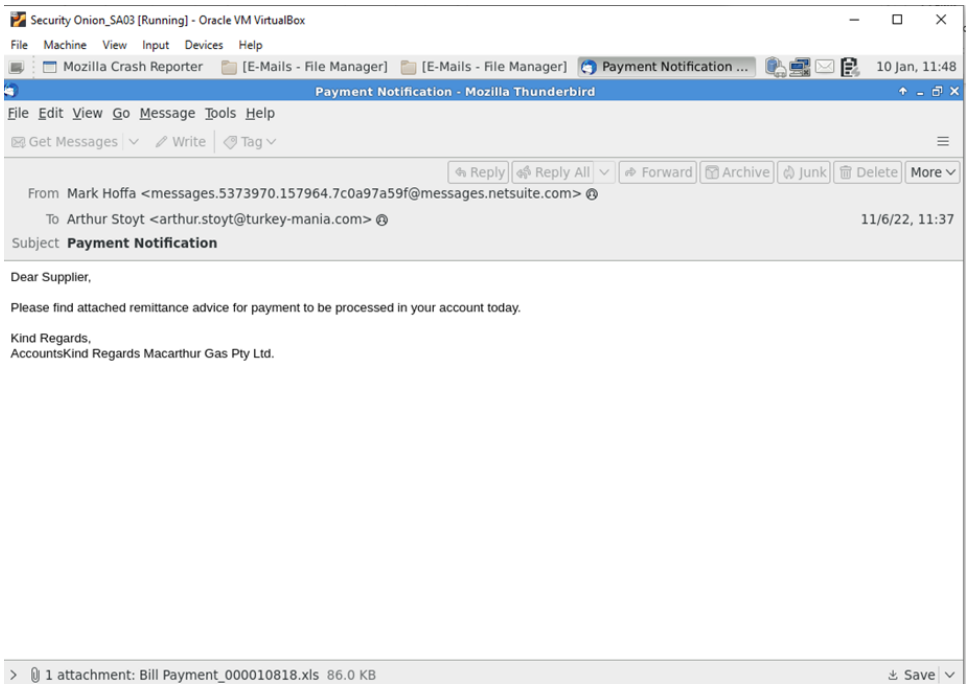
1. Login credentials entered into the login screen shown below.



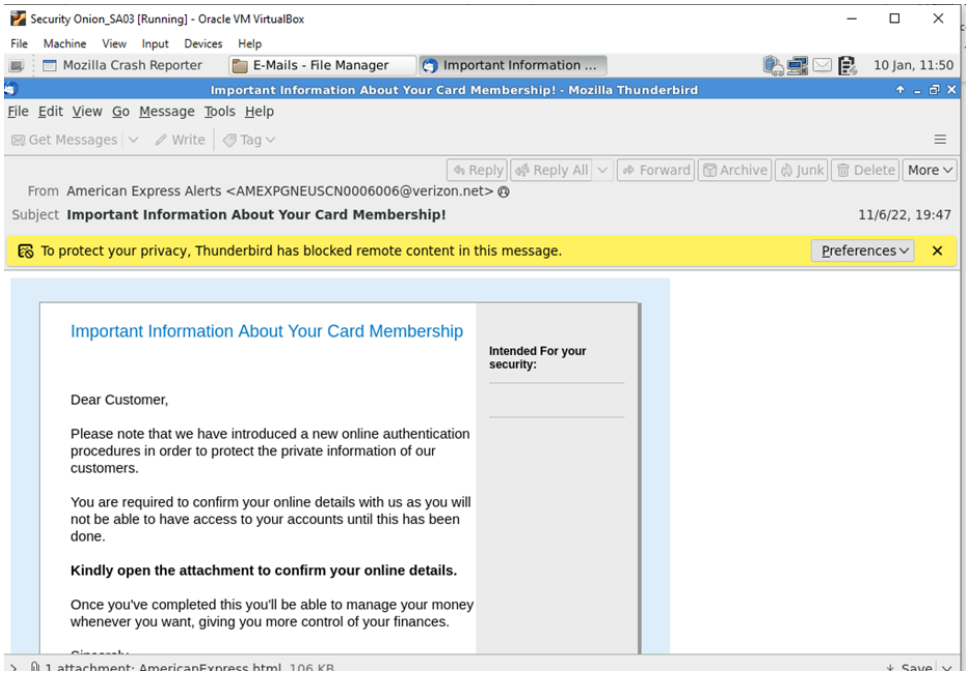
2. Email 01 opened successfully



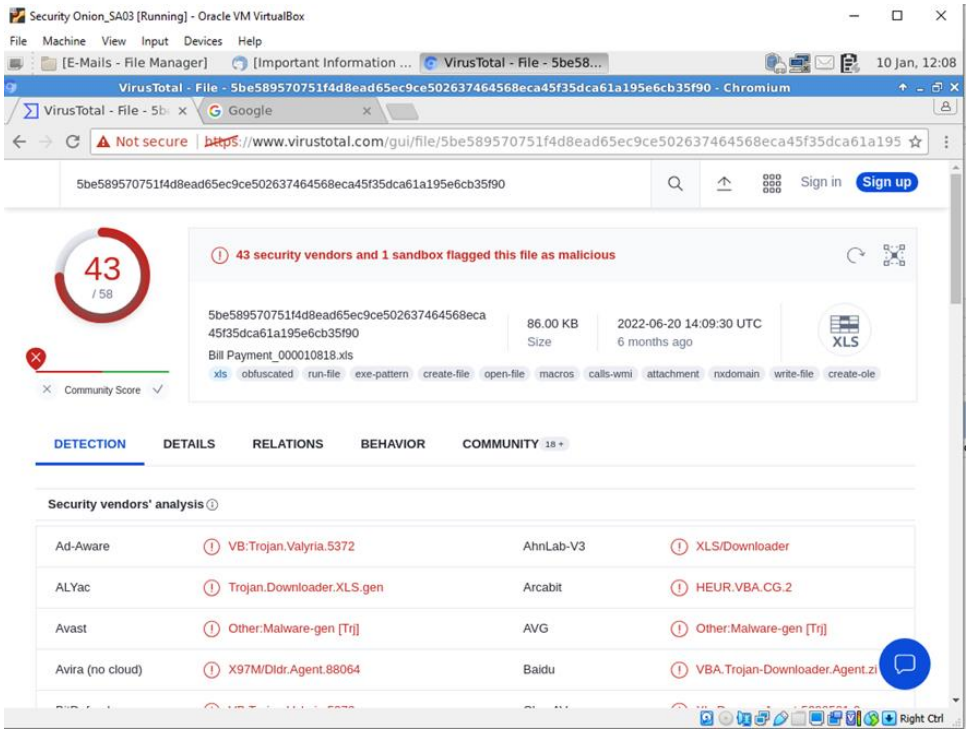
3. Email 02 opened successfully



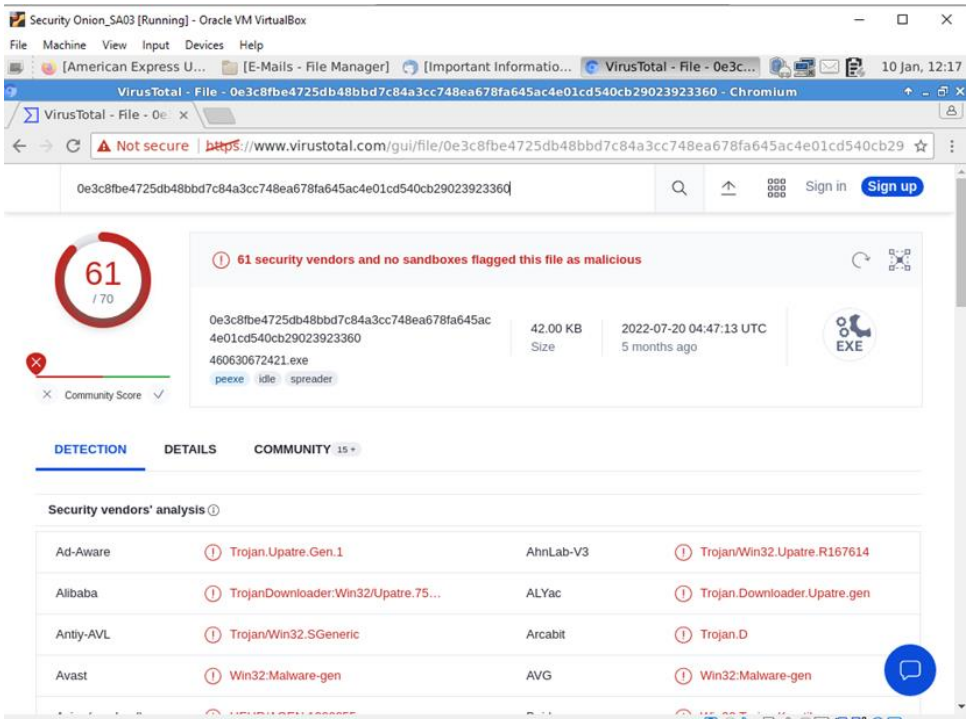
4. Email 03 opened successfully



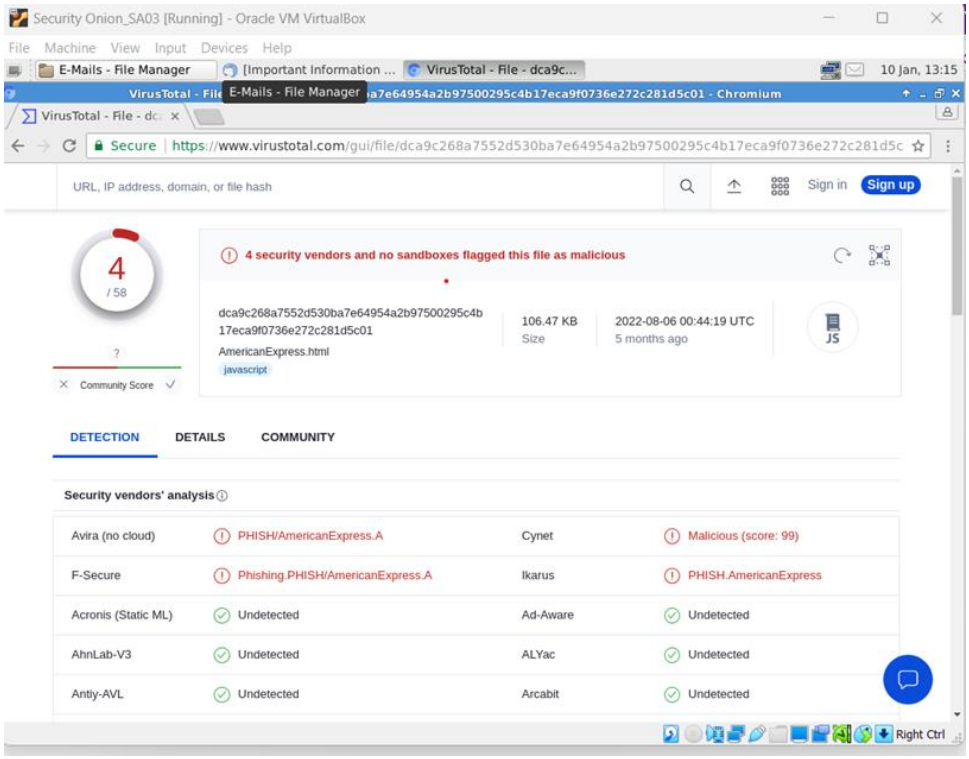
5. VirusTotal scan – Bill Payment_000010818.xls



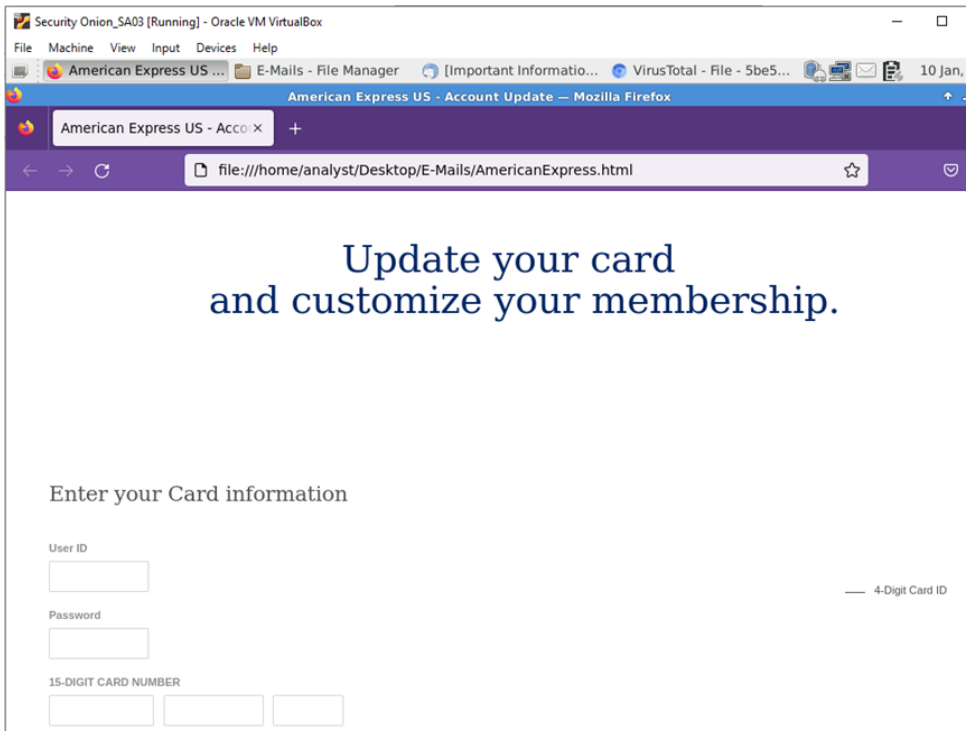
6. VirusTotal scan –460630672421.exe



7. VirusTotal scan results – AmericanExpress.html



8. Fake American Express page – AmericanExpress.html



Email Investigation and identification of any issues

I have studied the emails and will now present my findings; I will discuss each email separately.

Email 01 – Invoice 24887024 from Lockman, Gorczany and Cole

Email 01 has a link that does not work; this could be an indicator that the email is not from a legitimate source.

It also contains an attachment named dawning wall up.zip. Cybercriminals can use zip files to hide malware and distribute them through email or malicious links. Once the zip file is opened, the malware can be automatically executed and installed on the end device.

The zip archive contains an .exe file. Cybercriminals often use executable files to spread malware, viruses, trojans, ransomware, and spyware. Once the exe file has been executed, it can be installed and run on the end device, causing damage to the system or stealing sensitive information.

I uploaded the .exe file to the virustotal.com website and the results returned detailed the infection as a Trojan.

Email 02 – Payment Notification

This email has an attachment named Bill Payment_000010818.xls.

The XLS file type relates to a Microsoft Excel spreadsheet. I uploaded the file to the virustotal.com website and received results that informed me the file was infected with malware, the vendors flagged this as malware. The results detailed the infection as a Trojan.

The dangers of macro viruses are that they can be hidden inside office files and once the file has been opened it can take control of the end device. Some of the things that can potentially happen include opening backdoors, installing ransomware and spreading across the business network.

Email 03 – About Your Card Membership!

This email has an attachment named AmericanExpress.html.

I uploaded the AmericanExpress.html file to the virustotal.com website and the results detailed the infections as a phishing threat.

This HTML file is a fake login page for American Express and the page was crafted to request the victim to enter their credentials which would subsequently lead to these details being stolen through a social engineering attack.

Potential fixes

There are multiple ways that the company can combat and better prepare for future attacks on users' devices and data. Most commonly used is training in how to spot phishing emails and ways to ensure that these types of emails are stopped the second they reach a user within a business.

Part C The company should provide a way for users to block and report these emails as well as have a stronger filter on a user's inbox to further prevent this from occurring again. User training will be essential to protect the company from data being stolen, for example NCSC's cyber security training.

The following methods are recommended:

- clean Tony's laptop to ensure it is virus free
- update all malware software
- install latest operating system updates and patches
- run malware scans on all staff devices and clean if required

- run packet capture software to monitor network traffic
- configure firewall settings
- check all log files on servers to determine whether any suspicious activity has been logged

Future remediation

The following measures would reduce the risk moving forward:

- ensure all devices run anti-virus scans weekly
- check network traffic and alert when suspicious traffic is detected
- consider intrusion protection systems (IPS) that can malware that is attempting to be downloaded and block it
- consider a cloud email security solution
- consider a data loss prevention system that detects and quarantines anything that tries to send data
- look at access management currently being used to identify if there is a better solution, for example privilege access management (PAM).

The recommendations above would help in reducing any risks to the system.

Task 2: ongoing maintenance

Time limit

2 hours 30 minutes

Brief

Following the resolution of the issues identified in task 1, you have been requested to produce a report that evaluates how ongoing maintenance will ensure the network and systems will remain secure and effectively operational.

Instructions for students

Create an evaluative report that:

- recommends ongoing maintenance measures that could be implemented to ensure the system remains secure and operational – this should ensure that the issues encountered in task 1 do not occur again in future
- recommends any remedial action you would take to ensure these measures are implemented and justifies the approach taken
- identifies the additional requirements to ensure these measures are manageable
- explores any systems upgrades that might be required based on these measures

(18 marks)

Evidence required for submission to NCFE

Written evaluative report.

Student evidence

Identification and explanation of proposed remedial action

An examination of Tony's laptop highlighted some remedial actions that would be required to secure the laptop and other systems from attempts to compromise. This section seeks to identify the recommended remediation and explain what the remediation is in a non-technical way.

There are multiple ways that the company can combat and better prepare for future attacks on user's devices and data. Most used is training in how to spot phishing emails and ways to ensure that these types of emails are stopped the second they reach a user within a business. The company should provide a way for users to block and report these emails as well as having a stronger filter on a user's inbox to further prevent this from occurring again. User training will be essential to protecting the company from data being stolen.

Before anything is done, all affected devices need to be re-imaged and re-protected to clear them of any damage done by the viruses. Every device on the network will then be updated along with all software that is used to ensure that they are using the most secure versions. All users will then go through training on awareness of Phishing and other social engineering attacks that can occur. Resources will be created and shared for all users to have access to, as well as any links to additional websites and help. Processes can then be put into place so users can report these emails to the technical team and get them reported which can hopefully prevent this from happening more frequently.

Once this is in place, the business can now implement more business wide measures to protect users and devices. Things such as better tougher user access levels when it comes to emails and unsafe websites/links and downloads can help protect the users further. Wireshark can be used within the business to monitor all data packets that move between users on the network which can help the technical team better keep track of what users are doing and will put them ahead of future attacks. Along with Wireshark, intrusion detection can be used to give the company an edge over people trying to gain access to sensitive data within the network. This intrusion detector can allow the technical team to act more vigilant against any future attacks. Other software can be used such as better anti-virus scanners and monitoring can keep the network protected and constantly safe.

Data itself can be protected on a more personal level by introducing backups and user access levels to keep sensitive data more secure and only accessible by certain level staff. This could mean that an account that has been taken over by a hacker may not even have access to files they want due to these protective levels. Data backups mean that data that has been corrupted or lost by other means can be brought back in case of emergency.

The table below lists each of the potential systems upgrades along with an explanation of each:

Potential system upgrades and measures	**Explanation**
Schedule an anti-virus scan check on each laptop at least once per week as a minimum	The anti-virus installed on each laptop needs to be configured so that a scan is automatically carried out at least once per week
Install an intrusion protection system (IPS)	An IPS detects attempts to infiltrate a network by comparing traffic to known patterns of malware/exploits. It can then automatically block the attempted access
Install a cloud email security solution	A cloud email security system inspects incoming and outgoing emails scanning attachments for malware and

	automatically quarantining emails that are potential phishing attempts
Install a data loss prevention (DLP) system	A company's data is sometimes the most valuable asset it has. A DLP system detects, and quarantines attempts to send data out of the business so these can be investigated and blocked or approved
Implement privilege access management (PAM)	To do their daily work some network and system administrators need full administrative access to a system. In order to get this, they have accounts with full administrative access. If an attacker were to compromise their account this would give them full access and the ability to compromise a system very quickly

Evaluation of ongoing maintenance

The following ongoing maintenance is recommended:

Maintenance required	Recommended action	Justification
Vulnerability scanning and management	• implement vulnerability scanning of all assets • analyse and monitor scan results and determine remediation/patching required	Multiple new vulnerabilities are discovered regularly and if an attacker decides to 'weaponise' the vulnerability by writing an exploit a system breach could result. Using vulnerability scanning and management systems to look for these vulnerabilities, assessing what needs to be done to fix anything found and putting a process in place to ensure it will not happen again, removes the associated attack vector
Security patching	• implement a patch management system for each operating system type and create a test environment that allows monthly testing	Security patches are released by operating system vendors and application vendors to remediate any discovered security flaws in their products
Password policy	• implement a password policy with a minimum password requirement that is automated to force a change regularly	Passwords are the passport to accessing a company's systems so ensuring they are managed properly is essential. A password policy ensures that an agreed standard is met and adhered to by staff and should form part of their training

Examiner commentary

Overall, this student has been graded as a pass. Although they identify Tony's concerns, they lack detail, and the comparisons would have benefitted from further analysis. Throughout the report the student demonstrates an adequate understanding of cyber security and how this is evolving.

Task 1

I have given this student a pass because the student has stated the background to Tony's concerns but could have included more detail, and the comparison between malware and application issues is analysed well but lacks any detailed analysis of the wider impact of malware. The student completed a scan as requested but this could have included further analysis to support their findings. For example, they highlight that a file could be a risk and following the scan correctly identify any threats but do not discuss the virus scan in any more depth than this. This lack of further analysis would have missed other potential root cause findings.

The student showed a good understanding of the scan functionality of the anti-virus software, as well as a good understanding of the logical steps to take to analyse results. They showed an adequate understanding of the malware that was infecting Tony's laptop but the analysis lacks depth which demonstrates a surface-level understanding.

The student did not carry out a re-scan of Tony's laptop after the anti-virus software quarantined the malware showing a lack of understanding of the fact that malware can re-install itself when removed. The student showed a good understanding of the remedial action required, splitting it up by remediation target devices. The student showed an adequate understanding of the measures needed to reduce risk but only linked with Tony's laptop and not the potential threat to the wider IT infrastructure. The student showed an adequate understanding of the impact of the vulnerabilities on the business but missed some physical vulnerabilities such as tailgating and document theft.

Task 2

The student showed an adequate understanding of remedial actions and has identified re-imaging of devices and training of staff as they 2 key points. Although these are obvious methods further depth would have been appropriate here, for example it states, 'every device on the network will be updated....' but does not go into further relevant details. There is a table of potential systems and measures identified, which are all relevant, but again lacks further detail, for example anti-virus scanning to be scheduled at least once per week. Ongoing maintenance is highlighted through the included table which identifies recommended actions, but this is also vague in places for example 'forcing a password change regularly'. The student has an adequate understanding of how to show information in a clear format using tables, they have an adequate method of detailing the proposed remediation as well as a good way of explaining the remediation in non-technical terms with no acronyms. The student showed an adequate understanding of risk and the different risks that are linked to each attack type, they have an adequate understanding of what ongoing maintenance would be needed and a logical way of presenting the information.

Overall grade descriptors

Grade	Demonstration of attainment
Pass	The student is able to develop a project proposal to research and compare the current software available and justify their recommendations.
	The student is able to install supplied software onto a device and ensure it is all correctly configured.
	The student is able to identify and explain the difference between cyber attacks and software issues, and how a cyber attack could take place.
	The student is able to investigate the issues on the virtual machine provided and explain the most effective remedial action to take to mitigate any problems.
	The student is able to evaluate a network with regards to cyber security.
	The student is able to ensure that company resources and data are fully protected.
	The student is able to perform a security risk assessment of the site and the network.
	The student is able to recommend physical, administrative, and technical controls.
	The student is able to create a disaster recovery plan including recommendations in the case of service outages.
	The student is able to explain how remedial actions will protect the company, which includes considerations for security, manageability and upgradeability in relation to cyber security policies.
Distinction	The student is able to develop an in-depth project proposal to research and compare the current software available and comprehensively justify their recommendations.
	The student is able to install supplied software onto a device, demonstrating excellent capabilities in ensuring it is all correctly configured.
	The student is able to comprehensively identify and explain the difference between cyber attacks and software issues, and evidence a detailed understanding of how a cyber attack could take place.
	The student is able to thoroughly investigate the issues present on the virtual machine provided and fully justify the most effective remedial action to take to mitigate any problems.
	The student is able to carry out an in-depth evaluation of a network with regard to cyber security and identify areas of improvement.

	The student is able to perform an in-depth security risk assessment of the site and the network, identify areas of concern and give a rationale for each.
	The student is able to recommend physical, administrative, and technical controls and justify their recommendations.
	The student is able to create an in-depth disaster recovery plan, including justifications for recommendations in the case of service outages.
	The student is able to demonstrate in-depth knowledge and give a thorough explanation of how remedial actions will protect the company, which includes considerations for security, manageability and upgradeability in relation to cyber security policies.

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 Technical Qualification in Digital Support Services.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Published final version	June 2023	31 August 2023