T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

Assignment 2 – Distinction

Guide standard exemplification materials (GSEMs)

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

Internal reference: DSS-GSEM-17

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

Cyber Security

Guide standard exemplification materials (GSEMs)

Assignment 2 – Distinction

Contents

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 resolution.

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 cause applications to freeze and/or exit with an application error. These errors are recorded in the event log on Windows with full details of the faulting application/module and details of the error including an error code, another possibility could be related to corrupted files or accidentally deleted folders. With such files being corrupt basic computing processes could encounter errors or slowness.

A corrupted file could occur during power outages or if an issue has occurred during the saving of a file or unexpected program termination.

Malware infections on the other hand attempt to be covert so do not want anything they do to be recorded in logs. They look to get a ‘foothold’ on a computer and attempt lateral movement seeking a computer where they can escalate their privilege. This then gives them access to an account with permissions that will allow them to download other exploits and gain control of servers, workstations, and other devices. They can also attempt other compromises such as ransomware.

There are different methods that can be used to help determine the source of the issues.

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.

Vulnerability scanning is a useful source of information and can be used to verify vulnerabilities in a computer system. Areas that a vulnerability scan could identify include, open ports, unneeded running services, poor system configurations and missing passwords.

Network traffic analysers are used to view and monitor network activity that could identify rogue connections, IP addresses and any abnormal traffic flow for example data to and from unknown IP addresses.

Viewing log file evidence is a source of information that highlights system activity and can be used to see if there are any errors in log files for example the security section in Windows Event Viewer.

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.

Uninstalling and reinstalling the software that has been affected can be a good measurement tool, if the issues are no longer there after the reinstall then you have found the source of the problem.

Viewing Task Manager and system process information can highlight any system and hardware issues that may be linked to the software performance for example HDD/SSD issues, RAM problems and CPU problems.

Clean the registry, delete temporary files and remove installation files. Tools like CCleaner can be very efficient in achieving this and provide a good reporting feature to analyse results.

Check internal storage for unrecognised files and folders.

Check network configuration if accessing online services and data to gauge whether there are any unauthorised changes to network settings, ipconfig/all is a useful command for this task.

In summary, a cyber attack is the deliberate exploitation of a computer system and could affect the whole system. An internal software problem could be on a much 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 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.

Types of attack

The issue is most likely malware such as a virus, Trojan or worm because these types of infections are associated with the type of issues Tony is experiencing such as applications running slower than they used to, programs regularly freezing and not responding, and occasionally files not opening.

A virus is a specific type of malware that spreads itself once it is initially run; a macro virus is a common type.

A Trojan is a piece of code or a program that disguises itself as a legitimate piece of code or software; spyware is a common type of Trojan.

A worm is slightly different, a worm replicates itself to spread and infect other computers; it often uses a computer network to replicate and spread itself. Worms can have success on systems that contain security issues on the target devices to access it and deliver the payload.

How could this have occurred?

A macro virus infected Tony's machine when he opened an infected attachment.

A Trojan has been installed on Tony's laptop when he had run executed a file that was from an unknown/untrusted source.

A keylogger spyware program has been downloaded, installed and gone unnoticed when Tony has been using the internet or opening email attachments.

A drive-by-download attack by a malicious script being inserted into a web page Tony has visited.

A social engineering attack such as phishing; Tony may have divulged information or details at some point without realising it.

A brute force attack may have occurred where a dictionary file is used to attempt to crack Tony's password so the user could access the device and network, and potentially infect it.

A man-in-the-middle attack against unsecured WiFi connections when Tony logged into a public internet hotspot.

A cross-site scripting (XSS) injection of malicious code in a web application allowing access to Tony's browser cookies which could lead to an infection or sensitive information being stolen.

Part B

Investigation and analysis

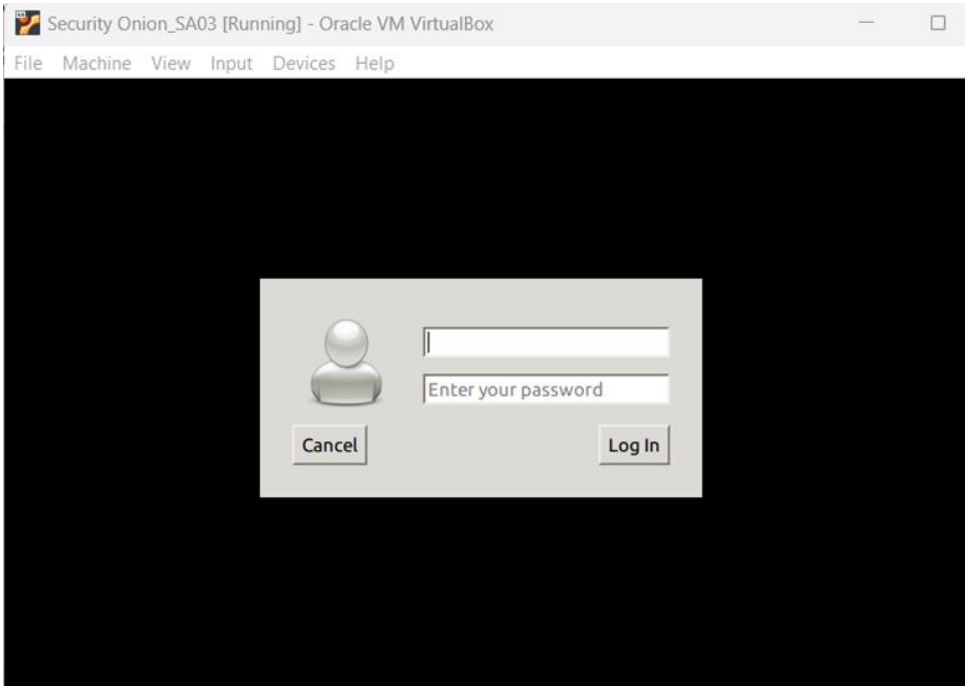
I have been given Tony's laptop to see if I can determine the cause of the issues.

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

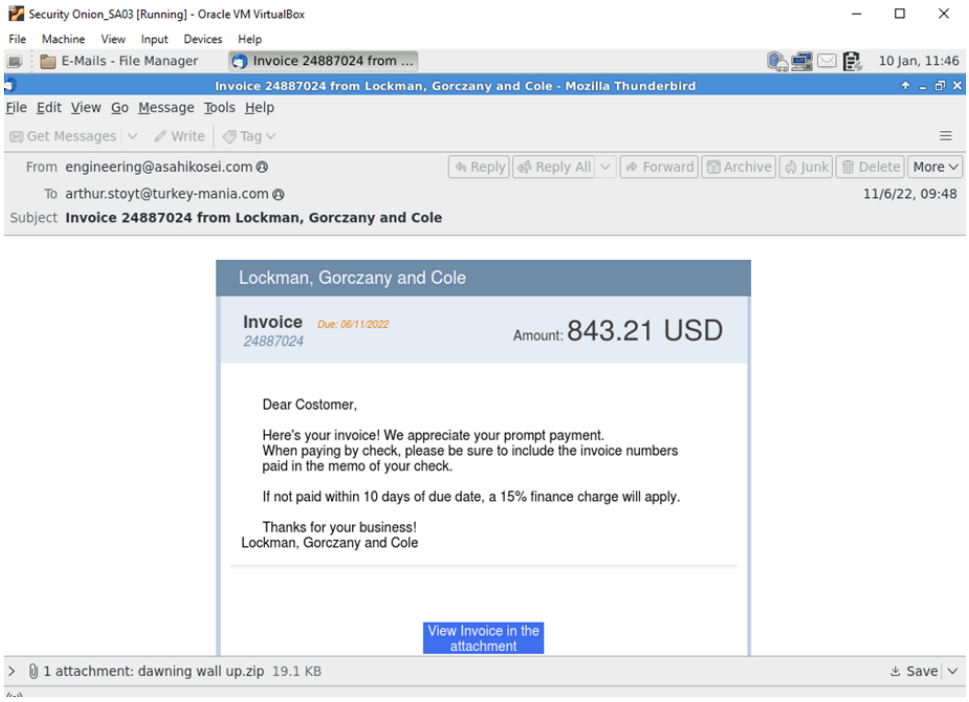
- using the credentials that have been supplied, successfully log into the machine
- analysing the emails that are on the device by opening them using the email client that is installed on the machine
- use the virustotal.com website to see if the email attachments contain any potential malware/viruses from multiple vendors.
- referencing any results against known vendor sites to see what information I can find about any infections that are highlighted.

Investigation

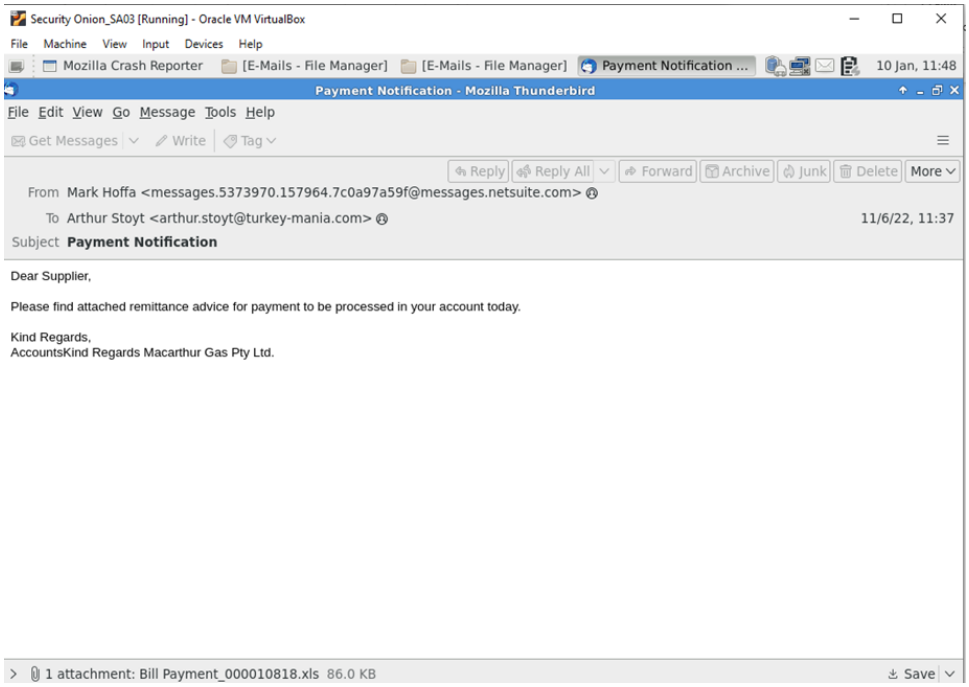
- successful login achieved; this is asking for the username and password and after entering this you can see the operating system running in the screenshot below



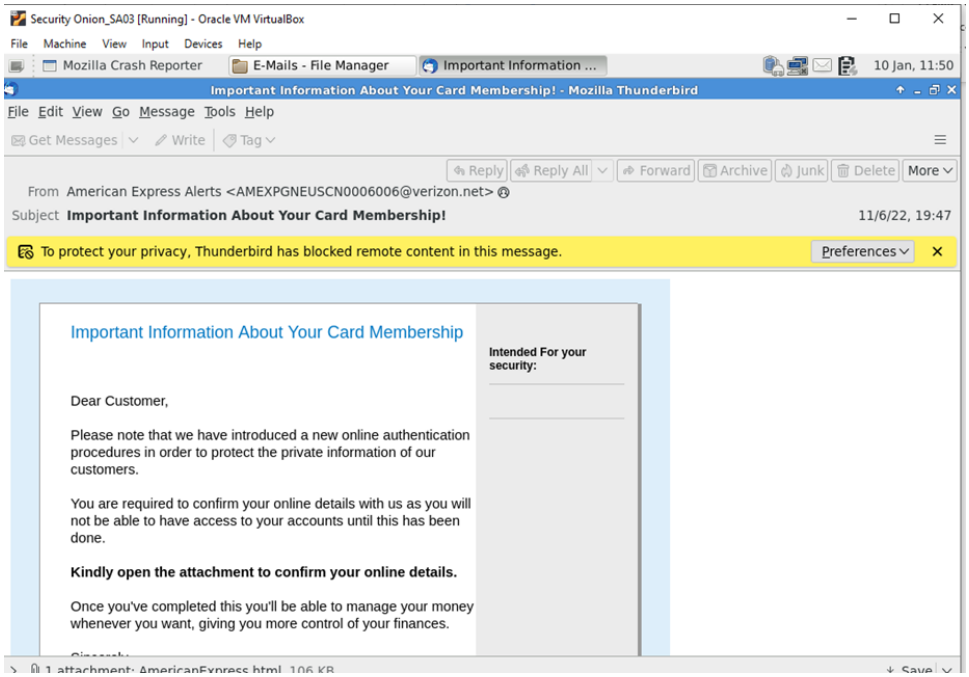
- email 01 opened successfully



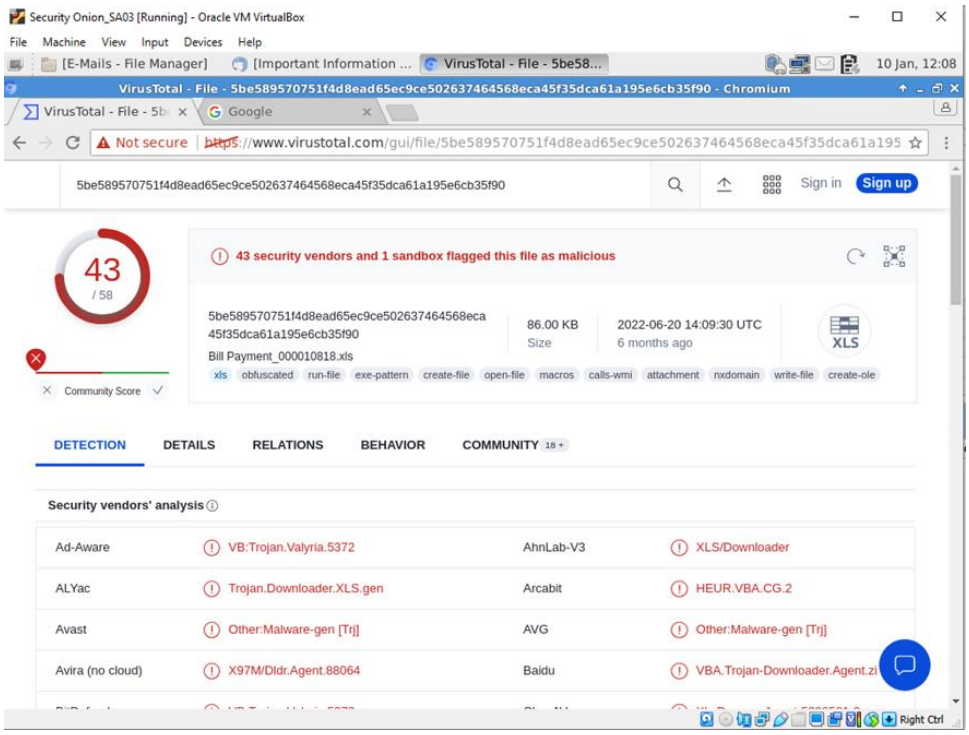
- email 02 opened successfully



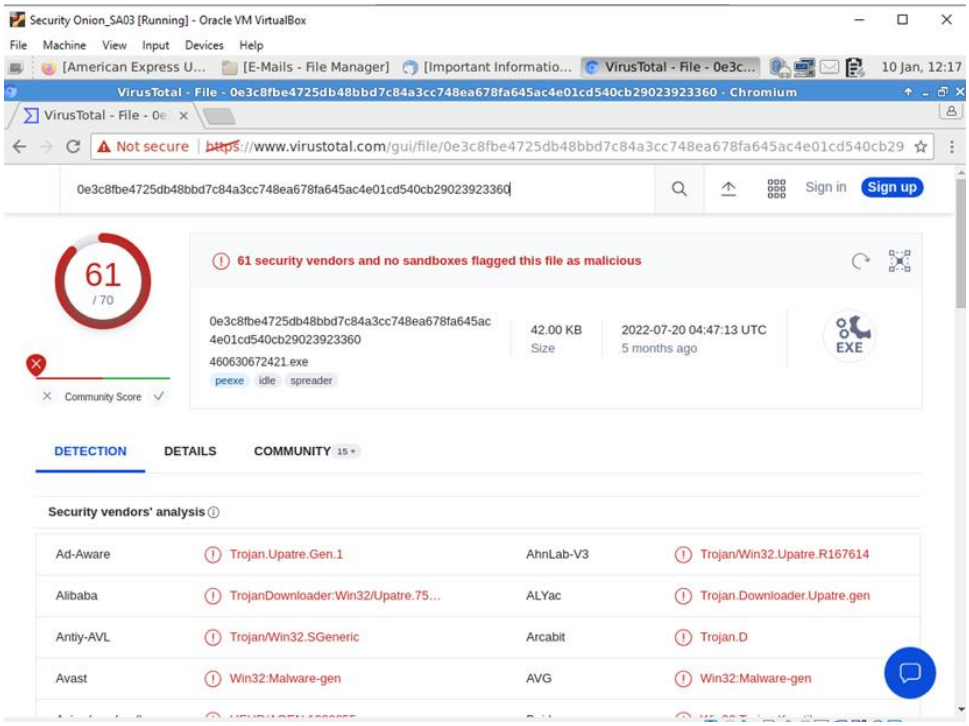
- email 03 opened successfully



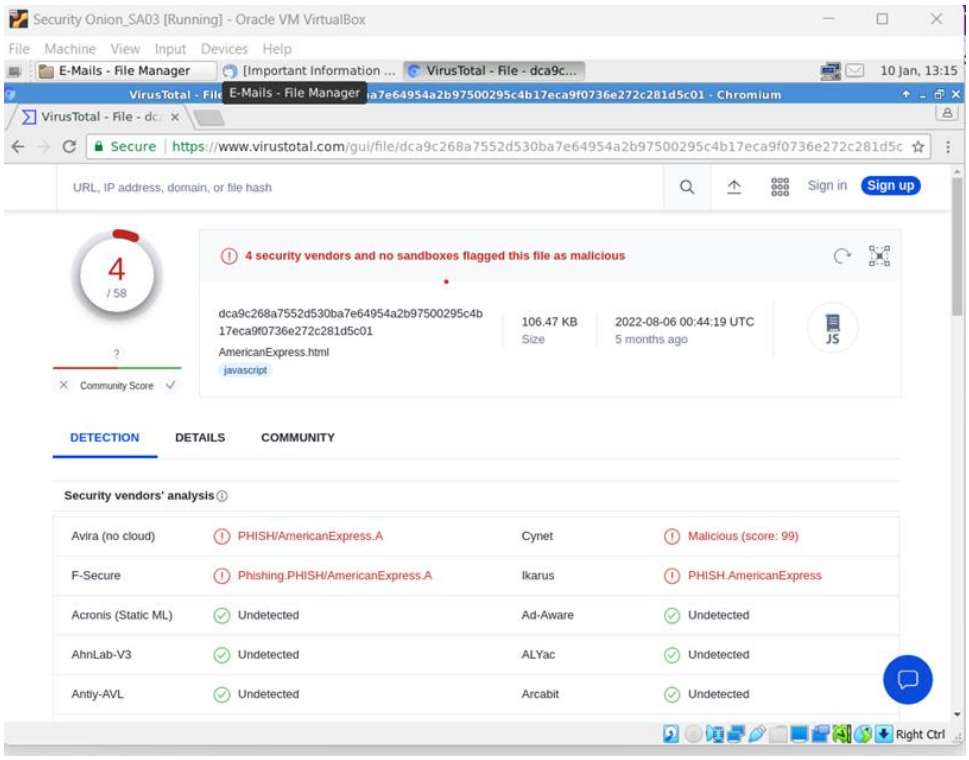
- VirusTotal scan – Bill Payment_000010818.xls



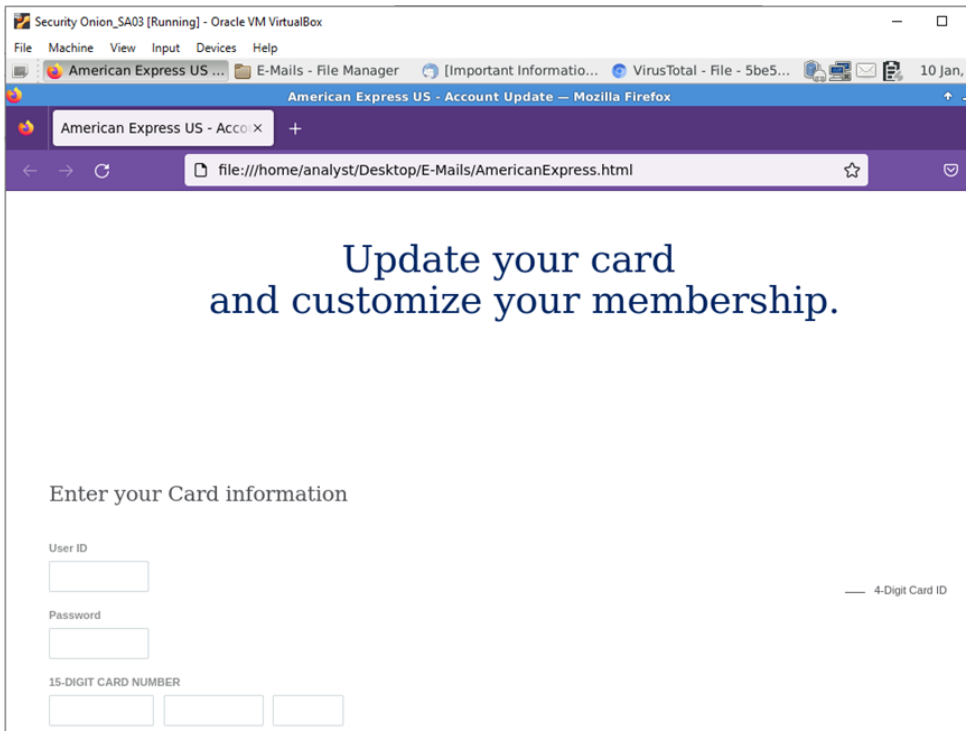
- VirusTotal scan –460630672421.exe



- VirusTotal scan results – AmericanExpress.html



- 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 is not an issue, but it can sometimes be an indicator that the email is rushed or not completed by a professional entity.

It also contains an attachment named dawning wall up.zip. Zip files can be a source of malware and if any of the files that have been zipped up in the archive contain malware, they will be restored to their previous infected state when unzipped.

The zip archive contains an .exe file which is potentially a malicious file type. Exe files are used predominantly on the Windows operating system but can be executed on other systems like Linux using specialist exe-running software such as Linux Wine.

Running executables that are email attachments is only advised if they are from a trusted sender or have been scanned by a malware program and if from an unknown source they should be discarded and possibly reported (according to policies and procedures in the business).

I uploaded the .exe file to the virustotal.com website and the results returned detailed infections found from 61 vendors; the main infection that was returned was a Trojan. Trojan is an umbrella term for an infection that can be present in a file, program, or piece of code that appears to be legitimate and safe but is malware.

Virustotal.com detailed the Trojan as Trojan.win32 and TrojanWin32.downloader as well as other Trojan variants. 'Downloader' refers to Trojan-Downloaders, a common type of Trojan Horse program that downloads and installs other programs onto a computer system, these programs can include keyloggers, backdoors, ransomware, and rootkits.

Email 02 – Payment Notification

This email has an attachment named Bill Payment_000010818.xls.

The XLS file type relates to a Microsoft Excel spreadsheet and other similar spreadsheet programs such as OpenOffice Calc or Apple Numbers. I uploaded the file to the virustotal.com website and received results that informed me the file was infected with malware, 43 vendors flagged this as malware. The results from the 43 vendors detailed the infection as a Trojan.

The dangers of macro viruses are that they can be hidden inside office files, and they are often written in Visual Basic/Visual Basic for Applications, the programming language used by Microsoft office products. Macro stands for macroinstruction, a set of programmed commands that will execute whenever a file is opened or when you perform a specified action to trigger prewritten code and subprocedures. This code can basically do anything such as delete files, open ports, change permissions and install malware.

One result returned from virustotal.com identified the malware as VB:Trojan.Valyria.5372; this infection is a Trojan written in VB and helps highlight the fact that it is a Trojan macro virus.

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 returned detailed the infections as a phishing threat. Only 4 vendors highlighted this as malware, one vendor identified this as PHISH/AmericanExpress.A.

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.

Fake login pages like these are not malware that would infect a Windows computer like a virus/Trojan/worm and may not always be picked up by malware scanners, but they are still a cyber security danger that is related to phishing and spear phishing and should be taken very seriously because they pose a very serious threat to an organisation.

This is quite an interesting tactic, feedback forms like the one contained in this email do not generally get distributed in this way, they are normally always displayed via a website as opposed to an email attachment.

Potential fixes

Two recommendations I would make to prevent this happening again:

- install malware / anti-virus software and schedule it to run regular checks on the machine
- train staff to raise awareness of information security and the identification of social engineering and phishing emails

The government has a department called the National Cyber Security Centre that provides information, templates, checklists and advice for businesses in the UK to help prevent cyber attacks and protect digital infrastructure, this could prove beneficial to a company like Willow.

Part C

There needs to be remediation at the asset/device level, network level and organisation level. Although most virus and malware scans could remove malware from Tony's laptop, the following is also recommended:

Asset/device level

- wipe and re-image Tony's laptop to ensure no other compromises are present that the anti-virus cannot detect, such as zero-day compromises
- update any malware scanners used in the business
- update all operating systems to conform with the latest updates/patches
- run malware scans on all assets to look for any further compromises
- re-image any assets that have an infection
- OS and device hardening
- disable macros on devices and in software packages where they are not required
- introduce email threat scanning, if not already present

Network level

- apply group policy rules to block executable downloads on the system and also to block users running executables that are not whitelisted for example Microsoft Word
- run a Wireshark packet capture on all network segments looking for suspicious traffic
- check firewall logs for any traffic going to unknown websites
- check that only the required ports are active for traffic and block at the firewall level if possible, for example, block port 20/21 for FTP
- update any intrusion prevention system (IPS) and intrusion detection systems (IDS)

- check all log files on servers to determine whether any suspicious activity has been logged
- check time and attendance records for staff and cross-reference to logs to determine whether activity has taken place against a login when the person is not at work

Organisation level

- run a communications campaign about the dangers of suspicious emails, this can be achieved through an email newsletter and posters
- provide staff training in cyber security awareness, for example, NCSC's cyber security training
- run a phishing campaign throughout the whole organisation to measure current understanding of the issues and use the results to plan for future training and cyber security awareness needs
- create a SharePoint site with additional cyber security information
- audit company cyber security policies to determine if they cover all required information

Future remediation

The following measures would reduce the risk moving forward:

- ensure all assets run anti-virus scans once per week as a minimum
- consider installing a network behavioural analysis solution to continually check network traffic and alert when suspicious traffic is detected for example command and control (C2)
- consider intrusion protection systems (IPS) that can detect the signature of a piece of malware that is attempting to be downloaded and block the download
- consider a cloud email security solution that detects and blocks phishing attempts
- consider a data loss prevention system that detects and quarantines attempts to send data out of the business so these can be investigated and blocked or approved
- consider a privilege access management solution (PAM) that controls the use of privileged administration accounts and prevents privilege escalation

The recommendations above would vastly reduce the risk of compromise to your systems and in doing so would vastly reduce the risk of data exfiltration from your systems.

Any data exfiltration could be in breach of GDPR, PCI DSS and other legislation/guidelines. It could also massively impact company’s reputation and potentially result in legislative penalties.

This would justify the adoption of the solutions outlined above.

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

For this report I will consider the issues that were encountered as part of task 1 and identify the types of vulnerabilities these could introduce to an organisation and the impact of this. For each of the vulnerabilities identified I will consider any countermeasures. By addressing this it will ensure the system remains secure and operational.

Vulnerability identification and impact

The following table looks at a range of physical and digital data security vulnerabilities, explains them and recommends any remedial action.

Vulnerability	Type	Countermeasure	Justification
Tailgating – attempts by unauthorised staff to gain access to a site by following a staff member who opens a door with a valid pass	Physical	• staff training • security barriers • pressure sensors	Tailgating results in unauthorised visitors onsite potentially performing reconnaissance for future attacks/stealing data. They could also be a physical danger to staff
Document theft – removing documents from desks or printer queues	Physical	• document retention policy • restricted document printing • security shredding • clear desk policy	Document theft could not only give a threat actor information they need to compromise security it could also result in adverse publicity and loss of confidence in the company if the data got to a publishing source. It could also result in potential legislative penalties and fines
Stolen ID – taking a genuine ID from a member of staff to attempt direct use or duplication	Physical	• staff training to report loss as soon as possible • biometric/pin pad secondary access • good quality photo for ID • time-based access restrictions, such as shift pattern only	Stolen ID can give access to a threat actor giving them the information they need to compromise security, potential adverse publicity, and loss of confidence in the company if the data got to a publishing source. It could also result in potential legislative penalties and fines
Malware/ransomware – malicious programs that attempt to infect machines allowing the attacker access or encrypt data then issue a	Digital	• robust firewalls • robust IPS/IDS • up-to-date anti-virus • network access control solutions	Malware/ransomware can be the entry point for a threat actor who can then build on this access to attempt data exfiltration/ransomware attack. These would lead to loss of reputation, financial loss or legislative measures

ransom demand to decrypt		• offsite/cloud data backup	
Outdated/unpatched software – software vulnerabilities are continually found and if the patch or fix issued by the supplier is not installed these could give a way to infiltrate the system	Digital	• vulnerability scanning solution • vulnerability management solution • robust patching/update process • patching automation system	Outdated/unpatched software can be the entry point for a threat actor who can then build on this access to attempt data exfiltration/ransomware attack. These would lead to loss of reputation, financial loss or legislative measures
Missing/poor data encryption – data transmitted (in-flight) or stored (at rest) should be encrypted so that if the physical media is stolen or an attacker 'listens in' on communications they cannot use the data as encrypted data cannot be read	Digital	• adhere to latest encryption standards • encryption at rest • encryption in-flight • secure sockets layer (SSL)/public key infrastructure (PKI) system	Missing/poor data encryption allows a threat actor to steal the raw data you keep on your systems and use for criminal purposes. This could include personal data or system data and could lead to legislative punishment/loss of reputation, financial loss or legislative fines

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.

The table below lists each of the proposed remediations along with an explanation of each:

Proposed remediation including system upgrades	**Explanation**
Schedule an anti-virus deep scan check on each laptop several times per week.	The anti-virus installed on each laptop needs to be configured so that a deep scan is automatically carried out at least once per week. This level of scan would detect more malware as it scans at a deeper level including operating system files
Install a network behavioural analysis solution	Sometimes a piece of malware installs itself on an asset and then uses the network to either replicate itself to other assets, allow the attacker access or send data to the attacker. A network behavioural analysis solution listens to and analyses network traffic looking for this type of behaviour and then identifies the assets

	that are producing the traffic. This allows those assets to be scanned and the malware removed
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. It also has the ability to upload new signatures as new exploits are discovered
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. A PAM system takes away full-time administrative access and only grants it when the system administrator needs the access, and usually this is linked to an authorisation process by a manager. This effectively renders their account the same as a standard user most of the time only giving privileged access on an authorised, time-bound basis
Implement server configuration for updates and multi-factor authentication (MFA)	Tools like Windows Server Update Server (WSUS) and Azure AD multi-factor authentication can be critical in keeping company devices up to date with the latest patches and also providing a secure authentication method for users
Schedule regular CPD for staff in cyber security awareness	Keeping staff fully aware of current trends in their day-to-day digital work is extremely important because threats can change very quickly, and this awareness could be the difference in whether a cyber security breach occurs

Evaluation of ongoing maintenance

Installation of the various controls is only one aspect of ensuring that systems are secure; there also needs to be a maintenance programme set up and adhered to. The following maintenance needs to be put in place:

Maintenance required	Recommended action and manageability	Justification
Vulnerability scanning and management	• implement vulnerability scanning of all assets • analyse scan results and determine remediation/patching required • pass a remediation plan including all remediation/patch management to the appropriate resolver groups	Multiple new vulnerabilities are discovered every week and if an attacker decides to 'weaponise' the vulnerability by writing an exploit (a code that leverages the vulnerability), a system breach could result. Using a vulnerability scanning and management system to scan all assets looking for these vulnerabilities, assessing what needs to be done to remediate any found and putting a management process in place to ensure remediation is done, will remove the associated attack vector
Security patching	• implement a patch management system for each operating system type • create a patch management process for any applications installed • create a patch management process where proposed patches are tested in a test environment for one month and then released to production on successful testing • ensure there is a reporting method in place to confirm patching was successfully completed	Security patches are released by operating system vendors and application vendors to remediate any discovered security flaws in their products. But there has to be a controlled way of releasing these patches that ensures they do not impact a system's stability or performance. Releasing to test then production allows patches to be tested avoiding these issues. Also ensuring all recommended security patching is applied as soon as possible ensures that any potential vulnerabilities in a system cannot be exploited by an attacker
Password policy	• implement a password policy with a minimum password requirement • minimum length • minimum complexity	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

	• force password change every 3 months • for privileged access also implement 2-factor authentication • passwords not to be written down • passwords not to be shared	staff and should form part of their training. Additionally, where users' accounts have privileged access, they should be secured with 2-factor authentication, for example a code from a smartphone authenticator application or a key fob
Penetration testing	• implement a regular penetration test by a 3rd party company • gather the results of the test and create a remediation plan for issues • carry out remediation • re-test to ensure all issues have been remediated	Putting controls in place can often give a company a false sense of security. A penetration test simulates an attack from a hacker and ensures that all controls behave as expected
Control audit	• audit all controls that are in place • this could involve attack simulation or even checks on policies and procedures • an example of this is sending staff a phishing email as a test and seeing how many click a link/supply personal details	Penetration testing will test your system's ability to hold up against an attack, but you also need to test your other controls and your staff's reactions. Regular phishing tests linked to training can help stop a potentially serious breach

Examiner commentary

Overall this student has been graded as a distinction as the work addresses Tony's concerns in full and includes an excellent comparison and analysis. Additionally, the report is well thought out and demonstrates an excellent understanding of cyber security threats and how these evolve.

Task 1

I have given this student a distinction because they have stated the background to Tony's concerns in full and have included a list of all issues, and the comparison between malware and application issues is analysed very well with an excellent analysis of the impact of malware on a computer and wider IT infrastructure. The analysis included the scan which was approached logically. Additionally, this benefited from network traffic analysis and viewing of log files as methods of further analysis. Screenshots were included but the flow of the report would have been easier to read if annotations have been more detailed at this stage. For example, there are screenshots of the emails being opened successfully but no further detail provided to highlight why that email could be a potential threat. The student has shown some understanding of Windows Event logging which includes the filtering out of events that were not part of the troubleshooting.

The student demonstrated an awareness of asset, network and organisational level remediation. This does provide an overview of activities that could be undertaken by the organisation for securing their systems. This included things like a network analysis tool (Wireshark) which could be utilised to analyse network traffic and identify suspicious activity. The student correctly identified particular port numbers, for example FTP. However, this can read a little generic at times and would have benefitted from a little more detail explaining this, for example, OS and device hardening. It would have improved the response to have seen an example for this. The student showed an excellent understanding of the scan functionality of the anti-virus software, as well as taking fairly logical steps to take to analyse results. However, the report could have been better structured making it easier for the reader to follow, for example after the student completed the scan it would have been good to have seen the results of the scan analysed against the infected file.

The student showed an excellent understanding of the remedial action required, splitting it up by remediation target devices and an excellent understanding of the measures needed to reduce risk, not only with Tony's laptop but also risks associated with the wider IT infrastructure. The student showed an excellent understanding of the impact of the vulnerabilities on the business including an exhaustive account of each vulnerability, its type, the countermeasures needed and the justification for applying countermeasures.

Task 2

An excellent understanding of remedial actions based on the vulnerabilities identified in task one. The student shows an excellent understanding and in places goes beyond the scope of the assignment brief, for example, the first table looks at physical vulnerabilities. Although these are not required in some instances the countermeasure identifies solutions that would be relevant to the scenario, for example the goal of the phishing attack is to gain information and the countermeasure of reporting as soon as possible would also apply to this. Overall, this section could have been focused more specifically on the scenario (the system).

The student provides a table of proposed remediation and system upgrades which provides a wide selection of options with a clear explanation for each which helps to demonstrate an excellent understanding. The student concludes with a table of ongoing maintenance and recommendations for how this would be actioned and managed. This is very detailed and clearly outlines the purpose and steps involved. Overall, this table shows an excellent understanding of security measure that could be introduced ranging from password policies through to regular penetration testing.

The student had an excellent understanding of how to show information in a clear and concise format using tables, they have an excellent method of detailing the proposed remediation as well as an excellent way of explaining the remediation in non-technical terms with no acronyms. The student showed an excellent understanding of risk and the different risks that are linked to each attack type, they have an excellent understanding of what ongoing maintenance would be needed and a logical way of presenting the information that is brief and to the point. There is a detailed table of vulnerabilities identified and their impact. However, the countermeasures though are bulleted points. If these had been expanded into a narrative, it would have helped to explain what the countermeasures are and how these would be implemented (it is the ‘how’ that would have benefited from further detail).

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