CSC3064 Case Study Assessment

Objective

You recently started a new job as an IT specialist at the Potayto Crisps company.

Potayto Crisps is a family-owned business that employs 40 people. The business is based at a single factory site, comprising a production line, a research department, and several other departments.

The company manager, Mrs Potayto, recently read about the threat of malware propagating via networks and is concerned about network security at the company's factory site.

You have been assigned a task to report back to Mrs Potayto with suggestions about how to configure the company's network infrastructure securely, including specific analysis and recommendations regarding the threat posed by 'Conti ransomware'.

You are asked to submit a short report that concisely presents your findings and recommendations.

This assessment is worth 60% of the available module marks.

You are required to submit a single pdf file, submitted via the Canvas *Assignments* page.

The submission deadline is 16:00 on 12 April 2022.

If you have a question about this assessment, email kieran.mclaughlin@qub.ac.uk

Background Information

The person in charge of managing the network at the Potayto Crisps company has recently retired. Mrs Potayto does not know all the details about the network at the site but has provided you with the following information.

- The factory site comprises a production line, a research department, a general administrative office, a sales and marketing office, and a small visitor centre. The offices contain several PCs and various other hosts, and all share the same network.
- The factory site uses a business broadband connection provided by an ISP. The network gateway used to provide access for the entire site is a Juniper Networks SRX110 device. The device was first installed around 6 years ago. Mrs Potayto says it seems to be working perfectly well and nobody has needed to make any changes to it since it was installed.
- The ISP provides up to four static IPv4 addresses. The gateway router has assigned one of the addresses to a NAT, behind which most of the internal hosts are connected via a switch. Another static IP address is used for remote access, described below. A third static IP address is used to host a booking website for the visitor centre.
- The gateway router is connected to a TP-LINK (TL-SF1048) 48-Port Unmanaged Switch, which provides wired connections to around 30 hosts across the factory site, plus additional wireless connectivity (Wi-Fi) through a Wireless Access Point connected to the switch.
- Mrs Potayto thinks all the hosts across the site share the 10.0.0.0/8 address range as a single LAN. The previous person in charge of the network said this was very convenient to allow employees to interconnect various new computers and devices across the site.
- The company has several unique and valuable recipes for crisp products, including their famous 'Onion & Cheese' flavour. The company values these recipes very highly. A Network Attached Storage (NAS) device from the vendor QNAP is used to share recipe data internally, and with external suppliers via NAT Port Forwarding settings in the gateway router.
- The research department is responsible for creating new crisps and monitoring the quality of crisps on the production line. The department uses a host running Windows Server 2012 R2, mostly for running "crisp quality analysis" software, which utilises live information from the factory floor. The network is configured to allow the supplier of the specialised analysis equipment to remotely log in using the Remote Desktop Protocol. This allows the external company to occasionally carry out maintenance and optimisation tasks to calibrate flavouring equipment in the factory production line.
- The factory has an on-site source of renewable energy generation that provides electrical power to the site. Management and configuration of the energy system is overseen within the general administrative office, using Siemens SICAM Toolbox II software.

Mrs Potayto has become concerned about network security after reading recent news articles about cyber-attacks. She has a special interest in the threat posed by '**Conti ransomware'** which affected the company KP Snacks in the UK.

Report Requirements

You must submit a report of ***1,500 to 2,000 words*** in total, including references. You should aim for 1,500 words, but do not exceed 2,000.

A concise technical report is required, not an essay. Use a reporting format and structure that delivers clarity. You should approach the report as you would for a real manager who is busy, and wants concise detail, clear reasoning, and clear advice, which can be quickly and easily understood and actioned.

Your report must have ***three sections*** as described below:

1. **Analysis of General Network Security Issues**
   - Consider the background information about the network and its usage, and present an analysis that identifies the key ***network*** security issues of concern at the company.
   - Your analysis should include justifications to explain why each issue you identify is problematic.

     For example, imagine we are analysing the condition of a house under construction. The observation, *"The lack of windows will allow water to enter. This will damage internal wooden fittings. It also enables access to the building, which poses a risk of theft…."* is more informative than simply stating *"There are no windows."*
   - You may wish to consider and evaluate the relative severity of each issue identified, and/or which issues should be addressed as a priority.

2. **Analysis of the threat posed by 'Conti Ransomware'**
   - Provide a summary describing the tell-tale signs and network-related 'Indicators of Compromise' (IOC) that might be used to prevent or detect the operation of the malware within a network.
   - Evaluate the risk posed by Conti Ransomware to the factory network, taking account of the specific properties of the threat and the general information provided about the status of the network and its usage.
   - Remember to focus on network-based IOCs. Much of the information available about Conti Ransomware will discuss encryption, file hashes, etc. which may not be useful from a networking perspective.

3. **Network Security Recommendations**
   - Propose how the security of the network can be improved, based on general best practice and your analysis of issues and threats from parts 1 and 2.
   - You should consider how to apply best practice security approaches to address network security regarding both ***detection*** and ***protection*** measures.
   - It is strongly recommended that you draw a network diagram, for example to illustrate how you would propose to configure the network to improve its security.

    - Be specific in tailoring security recommendations to take account of your analysis in parts 1 and 2.

      For example: *"Use a Network IDS to detect the presence of ransomware"* is much too general and does not address specific details of network-related features.

    - Where relevant, you should briefly explain and evaluate the effectiveness of your security recommendations, or any trade-offs.
    - Where information about the current network configuration is not known, state your (reasonable) assumptions and work from there.

In all sections you must focus on networking issues, not on operating systems or host software issues. For example, discussing executables is not generally related to networking (unless, for example, an executable can somehow cause activity that is observable on the network). Neither is hijacking a process, or encrypting local files, or discussing a buffer overflow via a code exploit (unless that can be seen in a network packet).

Referencing

You should include a small number of references to support key issues. Not every single source needs to be referenced. References count towards your total word count.

- Use no more than 6 references. Choose references related to key important issues.
- Provide your references as a footnote, like this[1]. Web links can be included as a URL. A formal referencing style such as APA or Harvard should be used for other types of sources.
- In the context of your report, effective use of a reference may be to summarise a key point from a source without the need to elaborate at length. However, the content of your report should be able to stand on its own – in real life your manager does not want to have to follow a bunch of references to fully understand your discussion!

Format

You may use any word processor to produce your document, but the submission must be a PDF. Use a simple document style and format (e.g. similar to this document you are reading).

- Your document style should be clear, uncomplicated, and professional.
- Font: Calibri, Arial, Times, or similar
- Font size: 11 or 12
- Do not use 1.5 or double line spacing to make the document seem longer.

[1] "Add footnotes and endnotes", https://support.microsoft.com/en-gb/office/add-footnotes-and-endnotes-bff71b0c-3ec5-4c37-abc1-7c8e7d6f2d78

Assessment Criteria

Your work will be assessed according to the indicative criteria provided as guidance below, and in accordance with the QUB Undergraduate Conceptual Equivalents Scale: https://www.qub.ac.uk/directorates/media/Media,837251,smxx.pdf

	80-100%	**70-79%**	**60-69%**	**50-59%**	**40-49%**	**0-39%**
Analysis of General Network Security Issues **[30% weighting]**	Outstanding exposition of wide range of network security concerns. Exceptional justification and explanation of findings. Strong judgments on severity of issues. Very strong insight focused on case-study details.	Excellent analysis of varied network security concerns. Insightful justification and explanation of findings. Very good judgments on severity of issues. Very good insight focusing on the case-study details.	Very good analysis of key network security concerns. Good justification and explanation of issues identified. Demonstrates judgment on severity of issues. A few prominent issues are overlooked.	Good analysis of key network security concerns. Some flaws in justification and explanation of issues identified. Relies on generic discussion of issues in parts. Could focus more on case-study details and networking.	Reasonable analysis identifying some key issues, but with gaps or misunderstanding. Lacks significant explanation of issues identified. Lack of focus on case-study details and networking. Overlooks major issues of concern.	Weak analysis, that overlooks several key security issues of concern. Misunderstanding. Does not engage with the case-study details.
Analysis of Conti Ransomware Threat **[20% weighting]**	Outstanding exposition of the threat. Highly informative analysis of the risk to the company network. Highly informative identification of network-based indicators of compromise. Identifies how to apply IOCs for network security with a very high degree of insight.	Excellent analysis of comprehensive range of network issues related to the threat. Strong analysis of the risk to the company network. Strong identification of network-based indicators of compromise. Identifies how to apply IOCs for network security with strong insight.	Very good analysis, covering a good range of network issues related to the threat. Very good analysis of the risk to the company network. Good identification of network-based indicators of compromise. Identifies how to apply IOCs for network security with a good degree of insight.	Good identification of several network issues related to the threat. Satisfactory analysis of the risk to the company network. Minor off-topic issues. Fair identification of network-based IOCs. Some IOCs are not network-based. Reasonable proposals to apply IOCs for security.	Mostly adequate identification of network issues related to the threat. Adequate analysis of the risk to the company network. Several off-topic issues. Identification of network-based IOCs is lacking. Several IOCs are not network-based. Proposals to apply IOCs lack depth.	Weak explanation with significant gaps and/or irrelevant material.
Network Security Recommendations **[30% weighting]**	Outstanding recommendations that would comprehensively address diverse issues. Exemplary justification and analysis of effectiveness. Exceptional use of external material. Strong insight focusing on the case-study details. Excellent diagram focused on the case-study.	Very good recommendations that would comprehensively address a breadth of issues. Excellent justification, including analysis of effectiveness. Highly effective use of external material. Substantial insight focusing on case-study. Strong diagram focused on case-study.	Very good recommendations that would effectively address identified issues. Clear justification. Reasoned analysis of effectiveness. Good understanding of external and module material. Good focus on the case-study, with few generic findings. Good diagram with only minor issues.	Good recommendations, with some gaps. Some justification. Unclear about effectiveness. Good understanding of module material. Relies too much on generic discussion rather than case-study details. Good diagram, but simplistic or generic.	Reasonable recommendations that would contribute to addressing identified issues, but with gaps or misunderstanding. Lacks significant justification. Lack of focus on case-study details. Lack of focus on network-related issues. Simplistic diagram, or diagram lacks explanation.	Weak or irrelevant recommendations. Misunderstanding. Lacks justification. Does not engage with the case-study details. No diagram or diagram poorly aligned with case-study.
Reporting style and organisation **[20% weighting]**	Outstanding reporting style. Professional levels of clarity and organisation of information. Outstanding use of a small number of references to support key issues.	Excellent and concise reporting style. Very well organised, exceptionally clear, and informative. Excellent use of a small number of references to support key issues.	Very clear reporting style. Organisation very good, but information could be more concise and easier to digest at a glance. Very minor flaws. Very good use of key references.	Clear style of reporting, but some issues with organisation. Could be more concise. Some room for improvement in organisation of information. Good use of references.	Clarity acceptable, but notable flaws. Not all information presented clearly. Lacks concision. Number of references too high, should prioritise issues to reference.	Does not adhere to document requirements. Word count too low/high. Lacks clarity. Disorganised. Information difficult to follow. Lacks references.

Assessment Aims

The broad aim of the report is to demonstrate and assess your ***depth of understanding*** across all the module topics, and your ***ability to apply*** that understanding to analyse and address a problem.

- You may wish to study and apply any of the lecture notes to help you, but you are also encouraged to look beyond the notes, particularly to support sections 2 and 3 of your report.
- Using external material to learn about an issue does not mean you need to reference every single source of information used to form your judgements – hence a maximum of six references is suggested. **References count towards your word count**.
- There is not a tick-box list of, for example, 20 items that you *must* identify in your report. However, you should aim to address a diverse range of relevant network security issues with a good depth of detail throughout.
- This is an open-ended investigation. Two students could submit very different reports and achieve an equally good mark.

Submission

You should submit your report as a **pdf** following the instructions in Canvas.

Plagiarism and Collusion

This is an independent piece of work and must be completed solely by you. You must not discuss or share your analysis with anyone else. The analysis presented must be your work, and your work alone.

By submitting the work, you declare that:

- I have read and understood the University regulations relating to academic offences, including collusion and plagiarism: http://www.qub.ac.uk/directorates/AcademicStudentAffairs/AcademicAffairs/GeneralRegulations/Procedures/ProceduresforDealingwithAcademicOffences/

- The submission is my own original work and no part of it has been submitted for any other assignments, except as otherwise permitted.

- I give my consent for the work to be scanned using plagiarism detection software.