DIGITAL & TECHNOLOGY SOLUTIONS
accredited by the Tech Partnership

Manchester Metropolitan University

Assignment Brief 2018/19
Unit Title: Computing Fundamentals
Unit Code: 6G4Z1902
Level: 4
Assignment Title: Computer Fundamentals Coursework
Unit Leader: Rob Hegarty
Contact Details: Office E128, John Dalton Building, Chester Street, Manchester Telephone: 0161 247 1541 Email: R.Hegarty@mmu.ac.uk
No of Elements in Assignment: 2
Submission Date: See date on Moodle
Submission Instructions: Submissions are to be made via the TurnItIn link on Moodle. Formative feedback will be provided in class, the feedback will help you to improve your mark. No grades will be provided until after the summative assessment has been submitted. Any student found guilty of cheating, plagiarising or seeking to gain an unfair advantage will face severe penalties. See the Student Handbook for further information.
Feedback Return Information: Feedback on the summative assessment will be provided within 4 weeks.

Assignment Task Overview

Scenario

Baron and Drew are a retailer of home cinema equipment. They sell a variety of products including televisions, speakers, amplifiers, Blu-ray/DVD players and cables. The company has its head office in Stockport and 5 retail branches around the UK (in London, York, Cardiff, Manchester and Newcastle) and a large warehouse in Birmingham.

Due to the specialised nature of the products, most sales are made in the shops, which also have demonstration facilities allowing staff to show off the products to customers before they buy. However, the shops can also take orders over the telephone. The company deals with a number of suppliers who deliver items to both the shops and the warehouse. Limited space is available in the shops, so large numbers of items are stored at the warehouse and sent to the shops when their stock runs low.

The company's buyer and stock controller are based in Stockport and work together to ensure that each branch has an adequate stock level of fast-selling items. If a shop takes an order for a product that it does not hold in stock, payment is taken and the item is sent to the shop from the warehouse. If the warehouse does not have a product in stock, it is ordered from the supplier by the buyer.

Computer Networks & Security

The primary aims of this project are to give you the opportunity to:

- Demonstrate how you can apply your knowledge of computer hardware, software, networking, and virtualisation to a synthetic real-world scenario.
- Carry out a brief vulnerability assessment and relate your findings to the main elements of computer security (Confidentiality, Integrity, Availability).
- Develop your understanding of access control, by restricting access to a webserver using UFW firewall.

Baron and Drew are venturing into online sales as way to increase their market share. As an established retailer of electrical goods, they do not want to risk damaging their reputation. For this reason, before commissioning a designer for the website they want to audit the security of their own in-house web server. Your task is to carry out this audit and demonstrate how you can mitigate some of the vulnerabilities you find in the system.

Overall Weighting

This assignments counts toward 50% of the unit mark.

Deliverables

In class multiple choice test – 40%
Report on Vulnerabilities – 30%
Report on Mitigation – 30%

Unit Learning Outcomes Assessed

2. Plan a simple computer network based on a business case study which includes security, data and traffic requirements.

3. Understand the function and role of a typical computer architecture

4. Appreciate and demonstrate awareness of security issues involved in information systems.

Apprenticeship Standard Learning Outcomes Covered

CSK1. Is able to critically analyse a business domain in order to identify the role of information systems, highlight issues and identify opportunities for improvement through evaluating information systems in relation to their intended purpose and effectiveness.

CSK4. Can undertake a security risk assessment for a simple IT system and propose resolution advice. Can identify, analyse and evaluate security threats and hazards to planned and installed information systems or services (e.g. Cloud services).

CSK7. Can plan, design and manage computer networks with an overall focus on the services and capabilities that network infrastructure solutions enable in an organisational context. Identifies network security risks and their resolution.

CTK6. Can identify common vulnerabilities in computer networks including unsecure coding and unprotected networks.

CB7. Applies analytical and critical thinking skills to Technology Solutions development and to systematically analyse and apply structured problem-solving techniques to complex systems and situations.

Negotiated Assessment

If you or your employer wish to pursue a negotiated assessment then your supervisor should submit a 1-2 page summary of the proposed alternative assessment to the Unit tutor listed on the cover sheet of this assessment.

In writing your summary please ensure that the learning outcomes listed on the front sheet of this assessment are covered and that the scale, complexity and level of the work proposed is broadly equivalent with this assessment.

It might be that you are working on a project in the right area but that the project you are working on is much larger or more complex than this assessment. In this case it might be possible to submit work which relates to part of the project you are working on, e.g. a subset of the functionality of a piece of software or similar.

If you are not sure of the suitability of an alternative assessment then your supervisor should speak directly with the unit leader, ideally by phone, so that they can quickly establish the feasibility of the negotiated alternative.

Assignment Details and Instructions.

You will conduct a basic vulnerability assessment on a virtual machine and put in place a firewall to mitigate some of the vulnerabilities you identified. Furthermore, you will make a recommendation on how to further secure the system.

Section A – Hardware, Software, Networking, and Virtualisation
Week Commencing 12/11/2018 in class multiple choice test. The test will cover the content of the unit up to and including week 7.

40 marks

Section B – Vulnerability Assessment
Explain what the Computer Misuse Act 1990 is and explain how the use of virtualisation can be used to prevent an accidental breach of the act during security testing.

Define what a port scan is explaining the goals and mechanisms employed by port scanners, ensure you fully explain how port scanners misuse the TCP three-way handshake.

Deploy the vulnerable web server virtual machine on a host only network, and carry out a scan against localhost. Report your findings specifying the number of open ports identified by your scan. Provide a screen capture to illustrate your findings (a photograph is not acceptable).

Access the CVE Mitre website (https://cve.mitre.org/find/) and lookup a CVE for two of the services you identified on the vulnerable virtual machine. Explain in your own words how the vulnerability could affect the confidentiality, integrity, or availability of the system, and what the implications would be for a business.

30 marks

Section C – Mitigation
Based on the results of your vulnerability assessment, you will have determined that there are a lot of open ports on the vulnerable virtual machine.

Research firewalls and explain how they can be used to increase the security of a computer system.

Research the use of UFW (Uncomplicated FireWall) and create a rule that filters one or more ports on the vulnerable virtual machine, ensure you leave port 80 open, and explain why. Provide evidence in the form of a screen capture of your UFW rules, and a screen capture of a port scan before and after, explain which port(s) you closed and why (photographs are not acceptable).

Other than closing unused ports, describe another approach to mitigating vulnerabilities in the system.

30 marks

Resources
The computers in the labs are required to carry out this assignment. Catch up sessions will be run periodically to ensure you have generated the screen captures required for evidence in your report.

Group Work Guidelines (If applicable, see Moodle)

Unit Specification – see Moodle

Assessment Marking Criteria

Grading Criteria					
Component	Fail (0 to 39%)	3rd Class (40 to 49%)	2nd Class: 2 (50 – 59%)	2nd Class: 1 (60 – 69%)	**1st Class (70-100%)**
Section A – In Class Test 40 Marks					
Section B – Port Scanning 30 Marks	A poor description of what a vulnerability assessment is, and incomplete description of the process carried out. Little evidence of working independently.	A fair explanation of what a port scan is. Some evidence of a port scan being carried out.	A clear description of how port scans work. An explanation of how virtualisation can help prevent accidental breach of the computer misuse act.	A brief explanation of the computer misuse act. A though explanation of port scanning. A brief explanation of virtualisation. A brief explanation of the TCP three-way handshake. Good evidence of a port scan. A clear original explanation of the vulnerabilities identified.	A thorough explanation of the computer misuse act, port scanning, and how virtualisation can prevent accidental breach of the act. A thorough explanation of the TCP three-way handshake, and description of how it is subverted by port scans. Well documented evidence of a port scan, and explanation of the vulnerabilities identified.
Section C – Mitigation 30 Marks	Little or no attempt made at mitigation.	A brief description of firewalls. Some limited documentation on the configuration of UFW rules. A limited description of other mitigation approaches.	A good description of firewalls. Documentation showing the firewall rules employed by UFW. Some evidence of the firewall functioning. A fair description of other mitigation approaches.	A detailed description of firewalls. A clear explanation of why port 80 is left open. An explanation of how UFW works. Evidence of a working UFW firewall. A review of alternative mitigation approaches.	A through explanation of what firewalls are and how they work. A fully documented and well-reasoned configuration of UFW rules. A comprehensive description of other mitigation strategies.