**NEWCASTLE UNIVERSITY**

ASSESSMENT 2023-24

**CSC8015 Cybersecurity**

Submission deadline: **23rd March 2024, 2.30pm**

Submit your completed answer to the questions via **NESS**, as a **pdf** document.

**Instructions**

Answer ALL questions

This assessment contributes 100% towards the total mark for this module. It is an individual exercise: no group work is required for the assessment.

Marks shown are indicative only

As for any University assessment, plagiarism will be considered as an assessment irregularity, and subject to disciplinary procedures. Please look at the guidelines:

<https://www.ncl.ac.uk/academic-skills-kit/good-academic-practice/plagiarism/>

In particular, be careful to cite properly bibliographic references. You can of course discuss your work with other students, but the work you submit must be individual.

Question 1 – Videos of attack demonstrations (40%)

**Learning Objective of the assessment**

As a security analyst, you must able to conduct concrete attacks on the system you are analysing, to test if some vulnerabilities are present or not. You must be able to use the relevant security tools and to develop the *adversarial mindset* (i.e., thinking as an attacker).

**Instructions**

The Canvas module contains a number of attack demonstrations you must perform and record. Your report must indicate the URL where the videos can be found (Stream, Youtube), one video per attack. The tools to be used for the attacks are covered in the lecture material.

Guidance on how to record your screen is provided on Canvas.

**Only a link to the video** will be accepted, please do not send us a video file.

* **Marking criteria for the video demonstrations**.
* **Success of the attack**. To score high marks, it must be clear from the video that the attack was successful as specified by the specification. Partial marks can be awarded for incomplete attacks if they are accompanied with an explanation of what does not work.
* **Clarity**: To score high marks, the video must be clearly presented, concise and focusing on the specific aspects of the attack.

**Question 2 – Security Analysis Methods (60%)**

**Learning Objective of the assessment**

As a security analyst, you must be able to design and justify an analysis strategy when considering a system, before actually conducting the attack. You must consider ethical and professional aspects and assess the potential effectiveness of the tools they want to use for a specific context.

**Instructions**

For each of the case studies below, design and justify a security analysis method in a report (**400 words max per report**). This report must be written as if you were asked by a client or stakeholder of a specific system to explain which security analysis method you would use for that specific system. Case studies might use systems and concepts not covered in the lecture material, thus mimicking the fact that no security analysist is aware of all systems existing in the wild. It is your responsibility to find information relevant to these systems. In some cases, you might have to make some assumptions on how these systems are organised or used. In this case, it is expected you will justify your assumptions based on your understanding of the context.

**Marking criteria for the analysis methods.**

Each report is marked individually, following a marking scheme divided in the following categories:

* **Risk Methodology**: To score high marks, the report should explain the risk methodology appropriate for the case-study, providing examples wherever appropriate.
* **Appropriateness of the tools**: To score high marks, the different tools selected should be the most appropriate to the case study.
* **Reflection on strengths/weaknesses**: To score high marks, the report should identify and assess the strengths and weakness of the proposed analysis method.
* **Awareness of the context**: To score high marks, the report should use material beyond the module relevant to the case.
* **Presentation**: To score high marks, the report must emphasise the key points, look professional, and be pleasant to read.

**Case study 1- Network Security**

A University is deploying a sensor network to transform their main building into a smart building, following the approach done at Newcastle University with the Urban Sciences Building and the Urban Observatory. <https://3d.usb.urbanobservatory.ac.uk>

More specifically, the University will deploy 1000 sensors across the building, which will be wired using the KNX protocol to BACNet controllers, connected to the main building management system using the IP network already present in the building. The main objective of these sensors is to capture CO2 to analyse how the building is being utilised.

Describe a method to analyse the security of this network of sensors.

**Case study 2: Web-application Security**

To facilitate the management of sensors, the University deploys a Web Server allowing to register a new sensor, to monitor the status of existing sensors. The server is deployed as a virtual machine in the Azure infrastructure managed by the University. Networking only allows access to this server from machines located within the local network of the University. The server is based on Ubuntu, with an Apache 2 server, running a MySQL database managed by PhP scripts.

Describe a method to analyse the security of this server.