FACULTY OF SCIENCE AND ENGINEERING
SCHOOL OF

Manchester Metropolitan University

UNIT CODE: 6G7Z1010	**UNIT TITLE:** Advanced Network Security	
ASSESSMENT ID: 1CWK50	**ASSESSMENT DESCRIPTION:** Report and presentation	**WEIGHTING:** 50%

School of Computing, Mathematics and Digital Technology

ASSIGNMENT COVER SHEET

COURSE: **MSc Cyber Security**
UNIT: **Advanced Network Security**
LECTURER: **Dr. Robert Hegarty / Dr. Thomas Martin**
ASSIGNMENT ID: **1CWK50**
ISSUE DATE: **January 2019**
HAND-IN DATE: ~~**12th April 2019**~~ **26th April 2019**

(after which maximum obtainable mark is 0%)

HAND-BACK DATE:
No responsibility is accepted by the School if an assignment is lost. To cover this eventuality, you are advised to take a photocopy of your assignment or to ensure you have the means of re-creating it.

PLAGIARISM: Students are reminded that plagiarism (copying) is a serious disciplinary matter. Checks are regularly made for misuse of the web and other existing materials. See Regulations for Undergraduate/Postgraduate Programmes of Study.

PROCEDURE FOR HANDING IN WORK: see Faculty Student Handbook. Follow any specific instructions given on the assignment specification.

PENALTIES FOR LATE HAND-IN: see Regulations for Undergraduate Programmes of Study.

EXCEPTIONAL FACTORS AFFECTING YOUR PERFORMANCE: see Regulations for Undergraduate Programmes of Study.
ASSESSMENT CRITERIA: see attached assignment specification.

FORMATIVE FEEDBACK

Verbal formative feedback will be provided during laboratory sessions, it is the student's responsibility to record and act on feedback.

Assignment description

This assignment aims to measure the following unit learning outcomes:

- Explain and critically analyse a variety of security attacks and propose appropriate security mechanisms to detect/prevent such attacks
- Use appropriate network development tools in the deployment of secure computer networks.

Assignment Tasks

1) Write a report (up to a max 2,000 words excluding the references and abstract) that describes the investigation you carried out into a vulnerable system.
2) Create and deliver a presentation on your investigation.

1. Overview

You will work to deploy a virtualised computer network. This will be used to demonstrate the use of ethical hacking techniques to appraise the security of a computer system. You will relate the security flaws found in the virtualised system to real world scenarios. You will compare empirical evidence from the virtualised system with primary, secondary and tertiary evidence from a variety of online resources. You will reason on and document how the empirical evidence is reflected in real world computer systems and historic security breaches. Your virtualised computer network will contain a vulnerable target system, and an industry standard attack platform (Kali Linux).

1.1 Report (85%)

Your report should include **the following subsections**:

1) Report title and your name(s).
2) Abstract
3) A table of contents
4) Introduction
5) Report Body (System deployment, Reconnaissance, Attack Analysis, Vulnerability and mitigation). Specifically,

- System Deployment: you will describe the architecture and configuration of the vulnerable system, and the precautions taken to ensure the vulnerable system and attack platform do not cause harm to the wider University infrastructure.
- Reconnaissance: you will carry out reconnaissance against the vulnerable target system, using the tools and techniques available in the attack platform. You will describe on the findings of the reconnaissance phase of the ethical hacking process. Describing any vulnerabilities you encounter, and their implications in a real world environment. You will research academic text, white papers, and news articles to illustrate the implications of the vulnerabilities identified.
- Attack Analysis: You will interpret the results of the reconnaissance stage of the ethical hacking process to identify vulnerabilities in the target platform. You will then formulate an attack plan by selecting appropriate exploits to target the vulnerable system. You will implement your attack plan and

document the success or failure of each exploit.

- Vulnerabilities and mitigation: You will provide a vulnerability and mitigation report for the system you analysed. The report will contain an overview of the process you employed to assess the system, and a description of how each of the vulnerabilities identified may be mitigated. You will refer to academic texts and other online sources and evaluate the solutions proposed and their ability to mitigate the vulnerabilities you identified.

6) Conclusion
7) References
In terms of formatting, the report should follow font “Times New Roman, size 11 or 12” and the citations should follow the Harvard reference format (Use Mendeley or similar to automate the generation of references)

1.2 Presentation (15%)
You will create a presentation describing your experience of the ethical hacking process from the beginning to the end. You will present the findings of your investigation and the proposed mitigation techniques to the class, and engage in discussion, about the implications of your report.

3. Assignment Marking Scheme

3.1. Report 85% (see the accompanying marking scheme for a more detailed breakdown of the allocation of marks).
3.2 Presentation 15%

4. What to hand in

You will need to submit your individual report through Moodle submission inbox, which is highlighted at the top of the unit Moodle area. You will need to submit your report as one PDF file. In addition please use the following naming structure for your report before uploading it to Moodle (“your lastname-firstname-studentID.pdf”).

NAME OF STAFF SETTING ASSIGNMENT: Dr. Robert Hegarty/ Dr. Thomas Martin

DOCUMENT UPDATED: 04/02/2019