FACULTY OF SCIENCE AND ENGINEERING
SCHOOL OF

Manchester Metropolitan University

COURSEWORK MARKING SCHEME

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

Marking Scheme

Structure	10%
Abstract	5%
Introduction	5%
Deployment	10%
Reconnaissance	15%
Attack	15%
Vulnerability & Mitigation	15%
Conclusion	10%
Presentation	15%
Total	100%

NAME OF STAFF PROVIDING MARKING SCHEME: Dr. Robert Hegarty / Dr. Thomas Martin

VERSION DATED: 11/09/2018

	Poor 0 – 39%	Acceptable 40 – 49%	Good 50 – 59%	Very Good 60 – 69%	Excellent 70 – 84%	Outstanding 85%+
Structure (10%)	Lacking logical structure. Lack of references.	Most of the main sections present. Little thought given to the structure of the work. References present but incorrectly formatted.	Main sections present. Adequate thought given to structure. Some references present.	Main sections present and correct use of headings and sub headings. Numerous relevant citations	All sections present with correct formatting. Numerous relevant references present.	All sections present, with correct formatting. Numerous relevant and up to date references present.
Abstract (5%)	Incomplete description/ summary regarding motivation/ ideas, approach and results of the report	Summary of most aspects, such as motivations/ ideas, approaches and the results of the report	Summary of the report in relation to motivations/ ideas, approaches and results of the report in all aspects	Good writing in relation to motivations/ ideas, approaches and results of the report	Excellence in writing the related motivation/ ideas, approach and results of the report	In addition to the elements found in the “excellent” criteria, the work shows creativity or ingenuity in work and expression and outstanding presentation of ideas.
Introduction (5%)	Incomplete and inappropriate explanation of the purpose of writing this report and indication of what the topic is about	Explanation of some points with few omissions	Good ability in explanation of the purpose of writing this report and an adequate presentation and indication of the topic, e.g., what's the motivation to do this topic. e.g. what your topic is, why it is important, and how you plan to proceed with your discussion	Well written explanation of the purpose of writing this report and a clear presentation and indication of the topic, e.g., motivations	Excellence in in explanation of the purpose of writing this report and an excellent presentation and indication of the topic, e.g., motivations	In addition to the elements found in the “excellent” criteria, the work shows creativity or ingenuity in expression and outstanding presentation of ideas.

System Deployment (10%)	Inadequate description of the threats posed by the use of the attack platform. A description of the system setup that lacks depth.	A fair overview of the system configuration. With limited information about the precautions taken and a deployment that departs from the provided specification.	A good overview of the system configuration, including explanation of reasons behind the system design. A fair description of the precautions.	A detailed description of the systems configuration, and justification for the system design choices. A good description of the legal and ethical issues.	A clear and insightful explanation of the system configuration and design choices. A thorough explanation of the legal and ethical issues.	A detailed and thorough explanation of the system configuration, including reasoning/ justification of design choices. A clear and coherent description of the legal and ethical issues surrounding the deployment of the system.
Reconnaissance (15%)	Incomplete analysis of the target platform carried out and poorly documented. Little reference to real world system vulnerabilities.	Partial analysis of the target system carried out and documented. Attempt made to relate vulnerabilities detected to real world systems.	Reasonable analysis of target system carried out and documented. A clear narrative describing the linkage between the vulnerabilities observed and their implications in the real world.	Thorough analysis of target system carried out, accompanied by a comprehensive report. In-depth analysis of the implications of the vulnerabilities observed in a real-world system.	Thorough and concise analysis of the target system. Accompanied by a comprehensive report critiquing the security of real-world systems exhibiting similar flaws.	A comprehensive analysis of the target system, citing multiple real-world studies into the prevalence and origins of the vulnerabilities detected in the target system.
Attack (15%)	Incomplete or inaccurate report that fails to identify relevant exploits.	Partially complete report containing a somewhat accurate attack plan, and reasonable attempts at applying exploits.	A reasonable report on the attack plan, with accurate identification of correct exploits (which include some obtained through independent research). Lacking detail.	A detailed and thorough report, clearly describing the process of identifying and leveraging the correct exploits (most obtained through independent research) for the vulnerabilities identified in the system.	A comprehensive report providing a clear and methodical approach to identifying vulnerabilities, and leveraging the exploits (all obtained through independent research) in the target system.	In addition to the elements found in the “excellent” criteria, a discussion on how novel exploits could be discovered.

Vulnerability & Mitigation (15%)	Incomplete or in accurate reporting of the systems vulnerabilities. Incomplete explanation of mitigation techniques.	Partially complete report, containing an in-depth overview of the systems vulnerabilities. A partial explanation of the mitigation techniques is provided.	A reasonable report on the system’s vulnerabilities, and identification of suitable mitigation techniques.	A detailed review of the systems vulnerabilities that clearly explains why particular mitigation techniques are suitable.	A clear description of the security vulnerabilities identified in the system. With a limited comparison of suitable mitigation techniques.	A precise and clear description of the system vulnerabilities. Critical analysis and comparison of a variety of mitigation techniques and strategies. Demonstrating a good understanding of a defence in depth approach
Conclusion (10%)	No closure and no stress on the main idea of the report statement.	Incomplete conclusion	Reasonable conclusion	Conclusion reinforces the main idea of the report	Excellence in reinforcing the main idea of the report and demonstrates the broader context of pen-testing	In addition to the elements found in the excellent area, the work shows outstanding grasp of theory and practice
Presentation (15%)	Incomplete or incoherent presentation of the investigation’s findings.	Partially complete presentation containing a limited overview of the investigation’s findings.	A reasonable presentation describing the key components of the investigation.	A detailed overview of the investigation and its findings. Giving detailed examples of the vulnerabilities discovered though independent research.	A clear and well-structured presentation on the investigation’s findings. With numerous high-quality explanations of the vulnerabilities discovered though independent research.	A thorough presentation of the investigation’s findings, critically reflecting on the investigation. Including a summary of the key points. Participation in Q&A with the class.