|  |  |
| --- | --- |
| **Programme:** | MSc Cyber security |
| **Module Code:** | LD7010 |
| **Module Title:** | Ethical Hacking for Cyber Security |
| **Distributed on:** | Via Blackboard; briefing in lecture. |
| **Submission Time and Date:** | To be submitted by 15:59 GMT on **20 May 2025** |
| **Word Limit:** | Part A - 60% (2000 words)  Part B - 40% (2000 words) |
| **Weighting** | This coursework accounts for 100% of the total mark for this module |
| **Submission of Assessment** | **Electronic Management of Assessment (EMA):** Please note if your assignment is submitted electronically, it will be submitted online via Turnitin by the given deadline. You will find a Turnitin link on the module’s eLP site.  It is your responsibility to ensure that your assignment arrives before the submission deadline stated above. See the University policy on [late submission of work.](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https:/northumbria-cdn.azureedge.net/-/media/teaching-excellence/pl,-d-,008-v005-late-submission-of-work-and-extension-requests-policy-stc.pdf?modified=20230401131943)  **Please note that assignments are subject to anonymous marking.** |

**Instructions on Assessment:**

This assignment consists of two parts

* Part A - 60% (2000 words)
* Part B - 40% (2000 words)

Any queries relating to this assignment should be directed to module leader: [baba.shaheer@northumbria.ac.uk](file:///C:\Users\wwjf6\Downloads\baba.shaheer@northumbria.ac.uk  )

**Assignment Details:**

For this module, summative assessment worth 100% of the total mark will be via this single individual assignment; to support evidencing achievement of all learning outcomes for the module, a written critical analysis report forms the basis of the module assessment. It is an individual assessment and should therefore be all your own work. Students should not collude or plagiarise work. Appropriate action will be taken, according to Northumbria University regulations, if collusion or plagiarism is suspected. Please see the section on academic integrity for clarification.

The purpose of this assignment is to perform and document a penetration testing phase as part of a practical ‘offensive security’ approach against a known network topology with distinguished characteristics and services. Furthermore, the report incorporates state-of-the-art research to demonstrate in-depth theoretical knowledge of a network security auditing paradigm regarding application and network layer attacks. You will learn how to defend a system and provide a better set of services in terms of security and availability and to further understand how planning and executing a set of steps and methods can seriously affect the security of a network.

**Mapping to Programme Goals and Objectives**

This assignment will assess the following learning outcomes:

1. Assess computer systems, information systems and networks to identify their vulnerabilities and weaknesses.
2. Evaluate and understand the principles of ethical hacking and appreciate where and in what situations these principles should be applied
3. Critically evaluate the core concepts, knowledge and practice of computer security have developed through research
4. Appreciate the legal and ethical issues associated with ethical hacking and be able to apply them appropriately.

# Important Information on possible Ethical and Legal Implications

Due to the nature of this module, you MUST ensure that ALL the attacks performed during the coursework are carefully contained within a controlled laboratory environment. The expected approach is to utilise virtual technology (e.g. VMware, Hyper-V and VirtualBox) to build your own lab.

Performing attacks on the virtual machines within the dedicated University laboratory is permitted, but it is very important to note that attacking the rest of the university network is NOT allowed. A full monitoring process will be in place and offenders could be prosecuted. Ask your module tutor to clarify any doubts shall you have further inquiries. Overall, make sure you comply with UK-legislation and all associated professional and ethical behaviour.

The purpose of this assignment is NOT to teach you how to break computer system but rather to understand how the countermeasures are applied to protect your potentially vulnerable infrastructure.

**Requirements**

For the practical part of this assignment, you will have to build three Virtual Machines (VM):

**A Linux Server**

* You could use CentOS or Ubuntu Server
* Minimum configuration required
* An additional service of your own choice (e.g. DHCP, FTP, SMTP, SNMP etc)

**A Client**

* Could be either Windows (Visa, 7, 8, 10 etc) or Linux (Fedora, Ubuntu etc)
* You could create multiple copies of the client’s VM if you require more clients to demonstrate an attack

**Attacker machine**

* [Kali Linux](https://www.kali.org/get-kali/#kali-platforms) (the most recent version is highly recommended)

**Module Specific Assessment Criteria and Rubric**

The work will be marked out of 100 in line with the University’s marking grades and according to the following assessment criteria:

|  |  |
| --- | --- |
| **Description** | **Marks** |
| **PART – A (60%)** | |
| Provide a summary of the configuration steps on the server and client. Include screenshots to evident functionality at the client-side. Discuss the rationale behind service selection and configuration. | 10 |
| Demonstrate a minimum of 2 attack against each of the two services configured. Any further and complex attacks will attract more marks. Log all the important and offensive events against your target including attacks detected, services’ logs nature, origin of the attack and damage caused. Support your demonstration with screenshots. | 35 |
| Critically reflect on countermeasures and prevention mechanisms applied to mitigate against your attacks. | 15 |
| **PART – B (40%)** | |
| In the second part of the report, you are required to write a short *position paper* to critically analyse and reflect on recent state-of-the-art attacks and hacking techniques, followed by a discussion on possible countermeasures. (weights 40%)  Your paper should consider the following guidance and contain the following subtitles as a minimum: |  |
| ***Title page and Abstract*** | 5 |
| **Introduction**   * An introduction using appropriate information and problem statement * The nature of the brief/commission and the topic should be briefly outlined and defined alongside details of how the paper is organised   **Scope:** How did you select the attacks/techniques in this paper? E.g. most recent attacks, wireless attacks, VoIP attacks, DNS attacks etc | 5 |
| **Main body**   * Critical discussion, reflection and analysis * Clear evidence of excellent critical thinking and problem-   + solving approach.   Excellent presentation in terms of communication and content. | 20 |
| **Conclusion**  A summary of the key findings established from your research. | 5 |
| **References** | 5 |
| *Marks deducted in case of poorly structured reports, layout, word count (15 marks)* |  |
| **Total** | **100** |

**NOTES ON PRESENTATION & SUBMISSION:**

The report must be written and presented to an appropriate academic standard for a postgraduate programme of study.

* The report will be assessed in terms of style, meaning, and the accuracy of spelling, grammar, punctuation, and syntax.
* The assignment should start with a Cover page including.
  + - Module: Ethical hacking for Cyber Security
    - Module Tutor Name:
    - Assignment title:
    - Student name + university identifier (always underline the surname/family name by which you are recorded in the university systems)
    - Programme or course of study:
    - Word Count:
* Your report written to a professional standard using MS Word and show appropriate and consistent use of type, fonts and line spacing (for this assignment use Arial 12 and single spacing) and page layouts. Give each page a footer that includes your name, the module code, and a page number.

**ASSESSMENT REGULATIONS**

You are advised to read the guidance for students regarding assessment policies. They are available online [here](https://www.northumbria.ac.uk/about-us/university-services/student-library-and-academic-services/quality-and-teaching-excellence/assessment/assessment-regulations-and-policies).

**Academic Misconduct**

The Assessment Regulations for Taught Awards (ARTA) contain the ***Regulations and procedures applying to cheating, plagiarism, the use of Artificial Intelligence (AI) Systems, and other forms of academic misconduct***.

The full policy is available [here](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https:/northumbria-cdn.azureedge.net/-/media/teaching-excellence/pl,-d-,005-v005-academic-misconduct-policy.pdf?modified=20230315105545)

You are reminded that plagiarism, collusion, the use of Artificial Intelligence (AI) Systems, and other forms of academic misconduct, as referred to in the Academic Misconduct procedure of the assessment regulations, are taken very seriously. Assignments in which evidence of plagiarism or other forms of academic misconduct is found may receive a mark of zero.

**Late submission of work**

Where coursework is submitted without approval, after the published hand-in deadline, the following penalties will apply. For coursework submitted up to 1 working day (24 hours) after the published hand-in deadline without approval, **10% of the total marks available for the assessment** (i.e.100%) **shall be deducted** from the assessment mark.

*For clarity: a late piece of work that would have scored 65%, 55% or 45% had it been handed in on time will be awarded 55%, 45% or 35% respectively as 10% of the total available marks will have been deducted.*

The Penalty does not apply to Pass/Fail Modules, i.e. there will be no penalty for late submission if assessments on Pass/Fail are submitted up to 1 working day (24 hours) afterthe published hand-in deadline.

Coursework submitted **more than 1 day (24 hours)** after the published hand-in deadline without approval will be marked as zero but will be eligible for referral. The reassessment should where appropriate, and as determined by the Module Leader, be the same method (e.g. essay) but maybe with a different task (e.g. different essay title) or with the same task (e.g. the same essay title) as indicated in the Module handbook.

In modules where there is more than one assessment component, Students are not required to complete all assessment components if an overall Pass Mark (40% UG, 50% PGT) has been achieved.

The only permitted exception will be in cases where the University is prevented from doing so by a PSRB requirement. In the case of PSRB requirements, a variation order will be required from the regulations.

In modules, where there is more than one assessment component and an overall pass mark has not been achieved, Students will be eligible for a referral\* in the individual failed module and/or not attempted component(s) of assessment.

These provisions apply to all assessments, including those assessed on a Pass/Fail basis.

The full policy can be found [here](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https:/northumbria-cdn.azureedge.net/-/media/teaching-excellence/pl,-d-,008-v005-late-submission-of-work-and-extension-requests-policy-stc.pdf?modified=20230401131943)

**Word limits**

The word count is to be declared on the front page of your assignment and the assignment cover sheet. The word count does not include:

e.g. appendices, glossary, footnotes, tables

Please note, in text citations [e.g. (Smith, 2011)] and direct secondary quotations [e.g. “*dib-dab nonsense analysis*” (Smith, 2011 p.123)] are INCLUDED in the word count.

If this word count is falsified, students are reminded that under ARTA this will be regarded as academic misconduct.

For those assessments where students are required to keep to the word limit, it is proposed that they should be informed that the marker will stop reading at the point when they judge that the word limit exceeds the recommended word count by more than 10%. The marker will indicate the point at which they stop reading on the text.

***Students must retain an electronic copy of this assignment (including ALL appendices) and it must be made available within 24hours of them requesting it be submitted.***

The full Word Limit Policy is available [here](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https:/northumbria-cdn.azureedge.net/-/media/services/academic-registry/documents/qte/assessment/guidance-for-students/pl013-v002-word-limits-policy.pdf?modified=20200803200335)

**Group Work**

The group work policy can be found [here](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https:/northumbria-cdn.azureedge.net/-/media/services/academic-registry/documents/qte/assessment/guidance-for-students/pl002-v001-group-work-assessments-policy.pdf?modified=20200804084402)