Assignment Specification
School of Computer and Engineering Sciences

Module Code	**Module Title**	**Assessment No**	**Weighting**
CO7607	Penetration Testing and Active Defence	2 of 2	30%

Title	**In-Year Reassessment Offered**	**Generative AI**
Offensive Countermeasures	No	Not Allowed

Summary	**Submission Date**	**Feedback Due**
This assignment requires students to explore and demonstrate the use of Offensive Countermeasures (OCM) within cybersecurity, including practical tool implementation and critical discussion of the legal and ethical implications of techniques like “hack back.” It combines practical work with academic theory, encouraging students to apply both practical and theoretical knowledge. The task reflects real-world challenges faced by cybersecurity professionals, particularly in penetration testing and active defence roles, where understanding attacker behaviour, legal boundaries, and ethical considerations is essential.	02/07/25 at 13:00 7-day Submission Window Allowed	04/08/25 13:00

Part 1: Offensive Countermeasures, Tools and Techniques (70%)

Offensive Countermeasures (OCM) generally helps us to defend ourselves against attackers and in the process, enables us to get a better understanding of who is attacking us and why. The general categories of OCM are Annoyance, Attribution and Attack.

A. Briefly research and explain, in your own words, each of these three OCM categories. Your discussion should include explanation of the category, its goal and how it can be accomplished. You may use examples.
B. Demonstrate the use of any three OCM tools, one for each OCM category. For each tool, you should identify the OCM category it belongs to. Provide an explanation of the tool e.g., what it is used for, how it may be used in a particular scenario and then demonstrate its use. For this you are to set up and use any two virtual machines of your choosing. One should play the role of a target whilst the other plays the role of the attacker. Configure and execute the tool as required. Use relevant screenshots, from both VMs, to document and explain the exercise.

Note: This section of the report should contribute 70% of the overall word count, i.e., 980 words. Higher marks will be awarded for high quality discussions which incorporate academic literature and references in APA7 format. The demonstration of the three OCM tools should be clearly documented, annotated and well discussed. **Please note that ALL terminal screenshots/figures** should clearly show your own individual assessment number i.e., J12345. No marks can be awarded without your J number being clearly visible. You may change this by using the below command on the Kali terminal.

sudo nano /etc/hostname

Part 2: OCM Arguments (30%)

Offensive Countermeasures (OCM), especially the idea of “hack back” or “self-defence” in cyber security, is a controversial idea and has stemmed some debate. There are multiple challenges here, on one side there are legal challenges whilst on the other moral arguments/dilemmas. Some make the argument that we should not be hacking back under any circumstances whilst others believe that we are within reason to take some sort of action to stay one step ahead of the attacks in the fight.

As part of this assessment, you are asked to research and discuss current UK legislation or legal status relating to OCM. Your discussion should address the following key points.

A. Summarise the arguments/debates around OCM, specifically arguments for and against the use of “hack back” and “self-defence” in cybersecurity.
B. Whether there is/are any existing specific legislation.
C. What you think is the general view on how the law on self-defence in cyberspace should be designed.

Note: This section of the report should contribute 30% of the overall word count, i.e., 420 words. Please note that higher marks are only awardable for higher quality and well researched discussions. Incorporating both professional and academic literature, all references and citations should be in APA7 format.

Additional Information

Learning Outcomes Assessed

- LO3: Demonstrate the use of some complex penetration testing and active defence tools
- LO6: Discuss the need for and uses of active defence
- LO7: Critically evaluate and analyse active defence techniques

Submission Window, Exceptional Circumstances, and Assessment Regulations

You are expected to submit work by the submission date specified at the start of the assignment specification. Some assignments may support a 7-day window in which students can submit work late without penalty and this will be specified below the submission date at the start of this brief. Any work submitted outside of the submission date (or submission window where allowed) will be given a mark of zero.

Academic Conduct

The material you submit must be your own work. You must not collude with your peers on your work unless the brief explicitly allows this (such as in the case of group work). The penalties for breaching the academic conduct policy are severe. The minimum penalty is usually zero for that piece of work. Further information is available.

Generative AI

The use of generative AI tools where not permitted will be treated as a breach of the academic c**onduct** policy.

This assignment **does not** permit the use of any generative AI tools, including but not limited to ChatGPT, Gemini, Copilot, Midjourney, and others.

Submission Information

- The final submission shall be 1400 words (with ± 10% flexibility), submitted as a Word or PDF document to Moodle via a submission link on the CO7607 Moodle page.
- An excess work count penalty of -5 marks per 1000 words excess will apply, e.g., if a 1000-word assignment, 5 marks deducted for 1101-2100 words).
- Permissible word count excludes the student's name, title of module and assignment, references to sources, bibliography, graphs, tables, maps, diagrams, captions and appendices.
- Please note, any work which is submitted elsewhere, other than via the turn-it-in link on the CO7607 Moodle page, will receive a mark of Zero and shall not be marked.
- The use of generative AI tools IS NOT PERMITTED and will be treated as a breach of the academic integrity policy.
- **Work submitted more than 7 calendar days late will NOT be marked and will receive a mark of zero.**

Assessment Criteria Postgraduate

Assignment Task (LOs Covered)	**Fail** (<50%)	**Pass** (50-59%)	**Merit** (60-69%)	**Distinction** (>=70%)
Part 1: Offensive Countermeasures, Tools and Techniques (70%) (LO3, LO6, LO7)	• Incomplete or inaccurate explanation of OCM categories. • Tool demonstrations are missing, flawed, or irrelevant. • Screenshots are missing or little evidence shown of tools being demonstrated. • Little to no academic references/citations in APA7 appear sources or referencing evident.	• Basic explanation of OCM categories with limited insight Tool • demonstrations included but may lack clarity or relevance VM setup • attempted with minimal documentation • Screenshots included but may lack context or annotations • Some use of academic sources with inconsistent APA7 referencing	• Clear explanation of OCM categories and their goals • Appropriate and technically sound tool demonstrations • VM setup and scenarios documented with reasonable clarity • Screenshots are present and well annotated • Good use of academic/professional sources, mostly correct APA7 format	• Insightful and wellarticulated discussion of • OCM categories Thorough, well-executed tool demonstrations • aligned to categories Clear and effective use of VMs with • welldocumented scenarios Screenshots are detailed and • generally very wellintegrated. Extensive use of quality sources with flawless APA7 referencing

Part 2: OCM Arguments (30%) (LO3, LO6, LO7)	• Discussion lacks coherence or misunderstands the topic • Legal and ethical considerations not addressed or otherwise misunderstood or incorrect • Arguments are unclear, one-sided, or missing • Little or no evidence of research or referencing	• Basic understanding of "hack back" and legal context • Some arguments presented but may lack depth or balance Legal • implications and legislation considered but perhaps not in • depth. Some academic/professional sources used with limited referencing accuracy	• Balanced discussion of ethical and legal debates around OCM • Demonstrates understanding of UK legal position and cybersecurity issues • Uses credible sources to support arguments • APA7 referencing mostly accurate	• Well-structured, critical analysis of OCM debates Insightful consideration • of UK law and wider ethical implications Strong use of relevant, • current literature from academic and professional sources Fully compliant with • APA7 referencing conventions