T1 2020 Assignment 1 Details and Submission Guidelines	
Unit Code	MN623 – T1 2020
Unit Title	Cyber Security and Analytics
Assessment Type	Individual Assignment
Assessment Title	Implementation and evaluation of penetration testing tools
Purpose of the assessment (with ULO Mapping)	This assignment assesses the following Unit Learning Outcomes; students should be able to demonstrate their achievements in them. a. Implement and evaluate security testing tools in a realistic computing environment
Weight	Assignment 1a - 5% Assignment 1b – 10%
Total Marks	Assignment 1a – 15 Marks Assignment 1b – 35 Marks
Word limit	Not applicable
Due Date	**Assignment 1a- Week 3, Thursday 5 pm, 9th April 2020** **Assignment 1b- Week 7, Thursday 5 pm, 30th April 2020**
Submission Guidelines	• Submit Assignment 1a in a word document in week 3. • Submit Assignment 1b in a word document and video presentation in week 7. • All work must be submitted on Moodle by the due date (week 3 for Assignment 1a and Week 7 for Assignment 1b) along with a completed Assignment Cover Page. • The assignment must be in MS Word format, 1.5 spacing, 11-pt Calibri (Body) font and 2 cm margins on all four sides of your page with appropriate section headings. • Reference sources must be cited in the text of the report, and listed appropriately at the end in a reference list using IEEE Transactions on Networking referencing style. • Students must ensure before submission of final version of the assignment that the similarity percentage as computed by Turnitin has to be less than 10%. Assignments with more than 10% similarity may not be considered for marking.
Extension	If an extension of time to submit work is required, a Special Consideration Application must be submitted directly through AMS. You must submit this application within three working days of the assessment due date. Further information is available at: http://www.mit.edu.au/about-mit/institute-publications/policies-procedures-and-guidelines/specialconsiderationdeferment
Academic Misconduct	Academic Misconduct is a serious offence. Depending on the seriousness of the case, penalties can vary from a written warning or zero marks to exclusion from the course or rescinding the degree. Students should make themselves familiar with the full policy and procedure available at: http://www.mit.edu.au/about-mit/institute-publications/policies-procedures-and-guidelines/Plagiarism-Academic-Misconduct-Policy-Procedure. For further information, please refer to the Academic Integrity Section in your Unit Description.

Purpose of the Assignment:

The Assignment1 focuses on implementing and evaluating security testing tools in a realistic computing environment. It helps the students to learn how to perform hacking/penetration testing. The students will demonstrate how a target system works, the weaknesses in the system, how to exploit those weaknesses and hack the system, and how to secure the system from the discussed weaknesses.

By doing this assignment, students will learn to evaluate and applies contemporary intelligent cyber security solutions for enterprise use which will definitely act as a stimulus for work integrating learning. By the end of the assignment, the students will have a strong base and a good understanding of hacking/penetration testing, so they can be able to combine the techniques learnt and tailor them to suit different scenarios. This assignment will be a stepping stone for the students to be work force ready for the booming cyber security industry.

Assignment Structure and submission guidelines:

Assignment 1 being formative assessment is divided into two parts. In the first part-Assignment 1a, focuses on hashes and passwords and implementation and evaluation of the major password attack tools available in Kali Linux that is marked for 5% of the total marks and the second part is an extension of first part along with understanding and implementation of Network Reconnaissance, Exploitation and Reverse Engineering security tools covering the remaining 10% of the total marks. In the second part- Assignment 1b, the students are required to explore and evaluate 3 security scanners but not limited to scanners like N-Stalker, Searchsploit and Metasploit tools. Students have to submit the first part by the Week 3, Thursday 5 pm, 9th April 2020. Once the first part is marked and a constructive feedback is provided, the responses to the comments/feedback has to be tabulated and appended to Assignment 1b that would be submitted by Week 7, Thursday 5 pm, 30th April 2020.

Kindly note the point 11. Academic Integrity mentioned in the Unit Description which is reproduced again for your perusal.

It is important to learn from the work of others and students are encouraged to explore the library, World Wide Web resources and have discussions with other students. However work for assessment must be entirely the student's own work.
Plagiarism can vary from minor lapses in referencing to the use of someone else's work or ideas passed on as the student's work without the origin of the material being appropriately referenced to serious breaches such as using someone else's work as one's own deliberately, recklessly and/or involving gross negligence.
Plagiarism—copying or using the work of others without giving details of the source of information—is not acceptable. All sources used and any collaboration in the exploratory work for an assignment must be clearly acknowledged using standard academic referencing.
Collusion, that is, secret cooperation between people in order to deceive others, is unacceptable. Contract Cheating, a form of collusion which involves employing or passing off work of any other person as the student's own work (e.g., paying another person to write the assignment), is a serious breach of academic integrity and has heavy penalties.

Students must not allow other students to copy their work and must take care to safeguard against this happening. In cases of copying, normally all students involved will be penalised; an exception will be if a student can demonstrate the work is his/her own and that the student took reasonable care to safeguard against copying.
Academic Misconduct is a serious offence. Depending on the seriousness of the case, penalties can vary from a written warning or zero marks to exclusion from the course or rescinding the degree. Students should make themselves familiar with the full policy and procedure available at:
http://www.mit.edu.au/about-mit/institute-publications/policies-procedures-and-guidelines/Plagiarism-Academic-Misconduct-Policy-Procedure

Assignment 1 Specifications

For this Assignment 1, you will implement and evaluate 2 password cracking tools in Kali Linux and explore and evaluate 3 security scanners.
You have to write a report for Assignment 1a and for Assignment 1b, a report with video presentation on how you will perform and evaluate these penetration testing tools is required.

Length of Video: The total length of the presentation should not more than 5 minutes (mark would be deducted for over-length presentation).

You may use any of the available open source software for screen capture. Please find the following as an example.

- **Software**:- http://camstudio.org/

Submission Guidelines:

1. Name your video with your student number and name.
2. Upload Video on your Youtube account
3. Copy the Video Link to a file (word document) and
4. Upload it into the MOODLE

To upload on Youtube, you must create your account on youtube. If you have a google account (gmail), you already have one on youtube. Videos must be of one of the following formats: .MOV, .MPEG4, MP4, .AVI, .WMV, .MPEGPS, .FLV, .3GPP, and .WebM. Once you have an account, to upload your video, click on the 'upload' button located at the top right-hand corner of your youtube.com webpage. To keep your uploaded video unsearchable by people so that random people cannot view your video(s), you have to select the privacy mode from the drop-down menu on the upload screen to be '**Unlisted**'. This way, your video is viewable by only those who have got the URL of your video. Make sure you copy and paste your video URL in the file submitted on MOODLE for your marker to be able to watch and mark it!

Marks will be awarded based on the sophistication and the difficulties in regards to the demonstration explored.

Assignment 1a: Implement and evaluate 2 password cracking tools in Kali Linux (15 Marks)

Focus on the following points while making a report:

• Demonstrate building a Software Test platform to evaluate 2 password cracking tools	5 Marks
• Why attack and Penetration Tools are important?	5 Marks
• What are the attributes of Good Assessment Tool for Penetration Testing?	3 Marks
• References	2 Marks

Assignment 1b: Explore and evaluate 3 Exploitation and Reverse Engineering security scanners.
(35 Marks)

Focus on the following points while making a video presentation and report:

• Addressing the feedback provided in Part 1 of the assignment	5 Marks
• Demonstrate understanding and implementation of Network Reconnaissance, Exploitation and Reverse Engineering security tools.	5 Marks

- There are several security scanners available in the market. Justify why you choose to explore the 3 Exploitation and Reverse Engineering security scanners you will be evaluating? 5 Marks
- The students will demonstrate how a target system works, the weaknesses in the system, how to exploit those weaknesses and hack the system, and how to secure the system from the discussed weaknesses. 5 Marks
- You should demonstrate 3 security scanners in the video and draw a conclusion on your experience with the 3 security scanners you evaluated. 8 Marks
- References 2 Marks
- Demo and Viva will be conducted in week 6 and week 7 lab classes. 5 Marks

Marking criteria:

Questions	Description	Marks
Assignment 1a	1) Demonstrate building a Software Test platform to evaluate 2 password cracking tools 2) Why attack and Penetration Tools are important? 3) Attributes of Good Assessment Tool for Penetration Testing	5 Marks 5 Marks 3 Marks
Assignment1 b	1) Addressing the feedback provided in Part 1 of the assignment 2) Demonstrate understanding and implementation of Network Reconnaissance, Exploitation and Reverse Engineering security tools. 3) There are several security scanners available in the market. Justify why you choose to explore the 3 Exploitation and Reverse Engineering security scanners you will be evaluating? 4) The students will demonstrate how a target system works, the weaknesses in the system, how to exploit those weaknesses and hack the system, and how to secure the system from the discussed weaknesses. 5) You should demonstrate 3 security scanners in the video and draw a conclusion on your experience with the 3 security scanners you evaluated.	5 Marks 5 Marks 5 Marks 5 Marks 8 Marks
Assignment1 b *Demo and Viva*	***Students remaining absent for Demo and Viva will lose 40% of the scored marks.*** *Demo and Viva will be conducted in week 6 and week 7 lab classes.*	5 Marks
Reference style	Follow IEEE Transactions on Networking reference style (should have both in-text citation and reference list) Minimum of 10 references for this Assignment 1a + Assignment 1b are a must. ***Note:*** The literature review should have minimum of ten journal/ conference papers (No blogs or Wikipedia to be considered) is required for both parts of Assignment 1. The reference papers used in this assignment need to focus on the recent research (last 2-5 years), but will also include older, more foundational papers for certain topics.	2+2 = 4 marks
	Total (Assignment 1a + Assignment 1b)	50 Marks

Marking Rubrics

Grades	HD	D	Credit	P	N (fail)
Assignment 1a	All the points are pertinent and covered in brief and provide good summary of the literature and activity performed in the assessment.	Mostly points are pertinent and covered in brief and provide good summary of the literature and activity performed in the assessment.	Many points are pertinent and covered in brief andprovide summary of the literature and activity performed in the assessment.	Few point are pertinent and covered in brief and provide outline of the literature and activity performed in the assessment.	Many points are not pertinent and not clear and summary is not provided for the activity.
Assignment 1b	Demonstrated excellent ability to think critically and sourced reference materials appropriately	Demonstrated good ability to think critically and but did not sourced reference materials appropriately	Demonstrated ability to think critically and did not sourced reference materials appropriately	Demonstrated ability to think critically and but did not sourced reference materials appropriately	Did not demonstrated ability to think critically and but did not sourced reference materials appropriately
Assignment 1a + Assignment 1b	All elements are present and very well integrated	Components with good cohesion	Components presented are mostly well integrated	Most components are present	Not adequately presented
Demo and Viva Voce	Understanding is clear and easy to follow with strong arguments	Good Consistent logical and convincing arguments	Some consistent logical and convincing arguments	Adequate cohesion and not satisfactory	Argument is confused and disjointed
IEEE Reference style	Clearly and completely followed IEEE style for citation (within) and references (at the end of) the document, number of citation is not accounted for.	Minor in-corrections but followed IEEE style for citation (within) and references (at the end of) the document, number of citation is not accounted for.	Some in-corrections but followed IEEE style for citation (within) and references (at the end of) the document, number of citation is not accounted for	Many in-corrections and not followed IEEE style for citation (within) and references (at the end of) the document, number of citation is not accounted for	No Referencing/ citation present at all