Dublin Business School
Assessment Brief

Assessment Details

Unit Title:	Computer Systems Security
Unit Code:	B9IS103
Unit Lecturer:	Pete Cassidy
Level:	9
Assessment Title:	CA
Assessment Number:	1
Assessment Type:	Written Report
Restrictions on Time/Length :	N/A
Individual/Group:	Group (max 3 students)
Assessment Weighting:	50%
Issue Date:	2nd Feb 2022
Hand In Date:	See Moodle page
Mode of Submission:	On-line via Moodle

Continuous Assessment Task

Weighting (50% of total mark for the module)

Report Max Word Count: 3500 words (Excludes diagrams, screenshots, command line input/output)

The assignment is an individual assignment.
Students must submit A SINGLE PDF Document

Part1: Setting up the Environment (15 Marks)

1. Within Virtual Box Manager setup a range of machines. Ensure they are on a host-only network environment.

2. Have at least 2 machines on the VM network:
Kali, DWVA
If you need the DVWA .iso file:
http://www.dvwa.co.uk/DVWA-1.0.7.iso

3. Familiarise yourself with the Kali Linux environment and its operation. Do the same for the other operating systems.

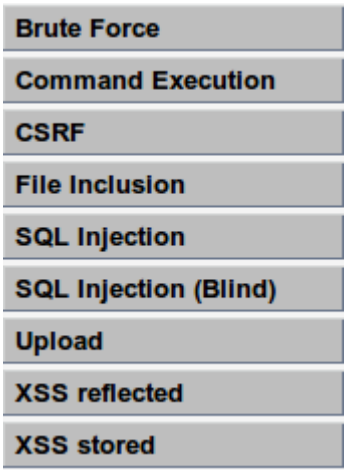
4. Ensure there is bi-directional communication between all VMs. Machines should all be accessible to each other on a single subnet (e.g 192.168.56.***)

5. For your report provide screenshots/diagram to demonstrate the setup. Be sure to provide ping and ifconfig screenshots from the VMs to show your setup is complete.

Part 2: Using the DVWA (30 Marks)

Demonstrate vulnerabilities on the DVWA server.

1. Pick one of the vulnerabilities within the DVWA.



2. Describe and demonstrate how the attack works.

3. Provide possible solutions for protecting against the chosen vulnerability.

Part 3: Demonstrate a Social Engineering Attack with Kali Linux (20 Marks)

https://github.com/trustedsec/social-engineer-toolkit

You are required to simulate a social engineering attack using the SET (Social Engineering Toolkit) in Kali Linux.

1. Perform a Website Cloning Attack. (Option 1-> Option 2 -> Option 3). Choose a website of your choice (the website should have a homepage which contains a login form/option (i.e. accepts a username + password via text boxes).

2. Have SET make a clone of the site, and harvest user information from the cloned site that the attacker could use to capture login details from an unsuspecting victim.

3. View and analyse the output report from SET to view the harvested data. For your report, detail what has occurred and use screenshots to accompany your answer.

4. Alternatively: discard steps 1 to 3... instead... Explain and demonstrate another attack of your choice from the SET.

Part 4: Presentation (35 Marks)

You are required to do a 10-15 minute presentation on ONE of the threats listed below. You are required to research your chosen threat to gather a strong technical understanding of how it works. Using diagrams/screenshots where appropriate, your presentation should detail:

● What the attack is.

● How the attack is performed (including technical details).

● Mitigation and Preventative Measures.

● How one can attempt to perform this attack using tool(s) within the Kali Linux environment. For this part, you should describe how the tool(s) would execute the attack in practice, using DVWA or an example website/webpage as a target.

Choose one of the following threats:

- Cross Site Request Forgery (CSRF)
- Reverse Shell / RAT
- Man in the Middle Attack
- Command injection
- Buffer overflow attack
- Password Attack (Brute Force or alternative)

(If you want to try an attack/defence other than those listed above, send me an email briefly describing your alternative. It should be possible to approve any reasonable alternatives)

Assessment Specification

Criteria/ Mark	< 40	40 - 49	50 - 59	60 – 69	70 +
Report	Difficult to read	Messy, needs tidying	Some errors and mistakes;	Few errors and mistakes	Presented excellently
Report Technical Data	Insufficient or incomplete	Some but insufficient and poorly structured code which doesn't solve the problem	Sufficient solves problem but lack of attention to detail	Well-structured that solves the problem	Excellent solution to problem

General Requirements for Students:

1. Save all your files in a folder and give it name: "Your Name". Compress the folder and upload it on Moodle.

2. It is your responsibility to ensure your files are uploaded correctly.

3. Students are required to retain a copy of their assignment.

4. When an assignment is submitted, it is the student's responsibility to ensure that the file is in the correct format and opens correctly.

5. Students should refer to the assessment regulations in their Course Guide.

6. DBS penalises students who engage in academic impropriety (i.e. plagiarism, collusion and / or copying). Please refer to the referencing guidelines on Moodle for information on correct referencing.

7. Extensions to assignment submission deadlines will be granted in exceptional circumstances only. The appropriate "Application for Extension" form must be used and supporting documentation (e.g. medical certificate) must be attached. Applications for extensions should be made directly to the Head of Year or Programme Leader in advance of the deadline date.