Final mark awarded:_____

Faculty of Computing, Engineering and Science

Assessment Cover Sheet and Feedback Form 2017-18

Module Code: IY1D402	Module Title: Cyber Security Tools and Practices	Module Lecturer: Clare Johnson
Assessment Title: Remote Exploitation		Assessment No. 1
No. of pages submitted in total including this page: Completed by student		Word Count of submission (if applicable): Completed by student
Date Set: 10-Nov-2017 15:00:00	Submission Date: 22-Dec-2017 23:59:00	Return Date: 19-Jan-2018 23:59:00

Part A: Record of Submission (to be completed by Student)

Extenuating Circumstances

If there are any exceptional circumstances that may have affected your ability to undertake or submit this assignment, make sure you contact the Advice Centre on your campus prior to your submission deadline.

Fit to sit policy:

The University operates a fit to sit policy whereby you, in submitting or presenting yourself for an assessment, are declaring that you are fit to sit the assessment. You cannot subsequently claim that your performance in this assessment was affected by extenuating factors.

Plagiarism and Unfair Practice Declaration:

By submitting this assessment, you declare that it is your own work and that the sources of information and material you have used (including the internet) have been fully identified and properly acknowledged as required[1]. Additionally, the work presented has not been submitted for any other assessment. You also understand that the Faculty reserves the right to investigate allegations of plagiarism or unfair practice which, if proven, could result in a fail in this assessment and may affect your progress.

Intellectual Property and Retention of Student Work:

You understand that the University will retain a copy of any assessments submitted electronically for evidence and quality assurance purposes; requests for the removal of assessments will only be considered if the work contains information that is either politically and/or commercially sensitive (as determined by the University) and where requests are made by the relevant module leader or dissertation supervisor.

Details of Submission:

Note that all work handed in after the submission date and within 5 working days will be capped at 40%[2]. No marks will be awarded if the assessment is submitted after the late submission date unless extenuating circumstances are applied for and accepted (Advice Centre to be consulted).

You are required to acknowledge that you have read the above statements by writing your student number(s) in the box:	Student Number(s): 17135397

[1] University Academic Misconduct Regulations

[2] Information on exclusions to this rule is available from the Advice Centre at each Campus

IT IS YOUR RESPONSIBILITY TO KEEP RECORDS OF ALL WORK SUBMITTED

Part B: Marking and Assessment
(to be completed by Module Lecturer)

This assignment will be marked out of 100%

This assignment contributes to 50% of the total module marks.

This assignment is bonded

Learning Outcomes to be assessed (as specified in the validated module descriptor https://icis.southwales.ac.uk/):

1) To demonstrate an understanding of the practices, principles, standards, legal and ethical issues associated with information assurance.
2) To demonstrate the ability to perform forensic and security incident management.

Feedback/feed-forward (linked to assessment criteria):

- Areas where you have done well:

- Feedback from this assessment to help you to improve future assessments:

- Other comments

Mark:	Marker’s Signature:	Date:

□ **Work on this module has been marked, double marked/moderated in line with USW procedures.**

Provisional mark only: subject to change and/or confirmation by the Assessment Board

Part C: Reflections on Assessment
(to be completed by student – optional)

Use of previous feedback:

In this assessment, I have taken/took note of the following points in feedback on previous work:

Please indicate which of the following you feel/felt applies/applied to your submitted work

- A reasonable attempt. I could have developed some of the sections further. □
- A good attempt, displaying my understanding and learning, with analysis in some parts. □
- A very good attempt. The work demonstrates my clear understanding of the learning supported by relevant literature and scholarly work with good analysis and evaluation. □
- An excellent attempt, with clear application of literature and scholarly work, demonstrating significant analysis and evaluation. □

What I found most difficult about this assessment:	
The areas where I would value/would have valued feedback:	

	Fail	Narrow Fail	3rd Class / Pass	Lower 2nd Class / Pass	Upper 2nd Class / Merit	1st Class / Distinction
Technical Summary and explanation of tools used 20%	□ No details on the target machine provided and no explanation of tools used	□ Very limited details on the target machine provided limited or no explanation of tools used	□ Basic / sufficient details on the target machine provided brief explanation of tools used	□ Good level of detail on the target machine good explanation of tools used	□ Very good level of detail on the target machine and detailed explanation of tools used some discussion on configuration of tools may be evidenced some alternative tools may be discussed	□ All relevant details on the target machine provided and presented in a clear and informative format, along with detailed explanation of tools used, configuration and alternatives
Password Recovery and explanation of tools / methods used 20%	□ No ability to recover the password no discussion of how this could be achieved	□ Unsuccessful attempt to recover the password limited or no discussion of how this could be achieved	□ Successfully recovered the password manually limited discussion on tools / techniques used	□ Appropriate tool used to successfully recover the password automatically clear explanation of tools / methods used	□ Well written script to successfully recover the password automatically clear explanation of tools / methods used, along with explanation of alternatives, difficulties encountered etc	□ Concise and accurate script presented, which successfully recovers the password automatically thorough explanation of tools and methods used and possible alternatives
Continued Access 20%	□ No attempt to maintain continued access to the target machine	□ Unsuccessful attempt to maintain continued access to the target machinelimited or no explanation of how this could be achieved despite being unsuccessful	□ Continued access to the target machine evidenced, but no attempt to conceal the detection of the continued access some explanation of how this could be achieved	□ Continued access to the target machine evidenced, with limited attempt to conceal the detection of the continued access sufficient explanation of how this was achieved	□ Continued access to the target machine evidenced some steps taken to conceal the detection of the continued access good explanation of how this was achieved	□ Continued access to the target machine evidenced excellent steps taken to fully conceal the detection of the continued access detailed explanation of how this was achieved
Proxy set up 20%	□ No evidence of proxy set up	□ Proxy set up is evidenced but unsuccessful limited or no explanation of techniques that could be used to do this	□ Proxy successfully set up and evidenced no attempt to conceal the detection of the proxy brief explanation of technique(s) used to do this	□ Proxy successfully set up and evidenced, but some steps taken are likely to be detectable sufficient explanation of technique(s) used to do this	□ Proxy successfully set up and evidence appropriate steps taken to conceal detection of proxy within the browser good explanation of technique(s) used to do this	□ Proxy successfully set up and evidenced appropriate steps taken to conceal detection of the proxy within the browser evidence is clearly presented and easy to follow detailed explanation of technique(s) used to do this along with evidence of configuration settings may include discussion of alternative methods
Report on Insider	□ No discussi	□ Very limited discussion on	□ Limited discussion on	□ Good discussion on	□ Very good discussion	□ An excellent discussion on

Threats 20%	on on insider threats	insider threats poor presentation	insider threats limited examples given writing style is difficult to follow and contains errors in spelling and grammar	insider threats with some examples given writing style is generally good with a few errors in spelling and grammar	on insider threats with good examples given writing style is easy to follow and coherent few or no errors in spelling and grammar	insider threats with relevant examples given writing style is concise and informative no errors in spelling or grammar

Remote Exploitation - Scenario

You are the Senior Technical Officer at eCorp, a company that designs and builds computer components. The Senior Management Team suspect that one of eCorps employees (Phillip Price) is exfiltrating intellectual property from the company, and have asked you to investigate their suspicions.

To do this, you have been asked to monitor Price's activities on the company network, and you have been given permission to use any appropriate methods of doing this, including scanning the network, by-passing the user's credentials, setting up a proxy to monitor traffic and so on. The company has provided you with a list of frequently used passwords which may be useful. Throughout your activities, you should make appropriate attempts to conceal the fact that you are monitoring this user's activities.

Once you have completed your investigation, you must write a report for the Senior Management Team, explaining exactly what you have done and what your findings were. You should discuss capabilities of the tools that you have used and explain whether any alternatives methods could have been used, along with any relevant configuration settings and examples.

In the final section of your report, you should explain what an insider threat is, what the implications are to an organisation, and give examples of where such threats have occurred. You should also discuss the implications of the tools you have used (along with other readily available tools) on the security of the organisation, and suggest methods for improving security in the future.

Hints:

You may find the following useful:

- Use a tool such as Nmap for the initial scan (Deliverable 1)
- Create a VM through which you can access Prices machine
- Write a Python script to attack the SSH on target machine. You will need to install an additional Python library such as pexpect which is part of 'expect' (Deliverable 2)
- Set up a method to permit you continued access to the target machine (Deliverable 3)
- Implement a proxy on the target machine and direct all web traffic through the proxy try to do this without notifying Price (Deliverable 4)

Deliverables:

Your submission should include the following:

1. Submit a preliminary report on Price's machine, providing details such as IP address, Operating System, Ports etc

2a. A python script used to attack the computer, along with screen shots showing that Prices machine has been successfully accessed

2b. A copy of the /var/log/auth.log file from Price's machine straight after cracking the password

3. A print out of the file: /etc/passwd on Price's machine

4. Evidence that you have set up a proxy to monitor traffic from Price's machine:

4a: Screenshots of the ip a output for both machines (clearly labelled)

4b: Wireshark *.pcap file from the client external adapter (NAT connector)

5. A report on insider threats as detailed above