|  |  |
| --- | --- |
| ***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]](#footnote-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]](#footnote-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): |

**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.* |

**Marking Scheme**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Fail  0-29 | Narrow Fail  30-39 | 3rd Class / Pass  40-49 | Lower 2nd Class / Pass  50-59 | Upper 2nd Class / Merit  60-69 | 1st Class / Distinction  70-100 |
| Technical Summary 25% | * No details on the target machine provided | * Very limited details on the target machine provided | * Basic / sufficient details on the target machine provided | * Good level of detail on the target machine | * Very good level of detail on the target machine | * All relevant details on the target machine provided and presented in a clear and informative format |
| Password Recovery 25% | * No ability to recover the password | * Unsuccessful attempt to recover the password | * Successfully recovered the password manually | * Appropriate tool used to successfully recover the password automatically | * Well written script to successfully recover the password automatically | * Concise and accurate script presented, which successfully recovers the password automatically |
| Continued Access 25% | * No attempt to maintain continued access to the target machine | * Unsuccessful attempt to maintain continued access to the target machine | * Continued access to the target machine evidenced, but no attempt to conceal the detection of the continued access | * Continued access to the target machine evidenced, with limited attempt to conceal the detection of the continued access | * Continued access to the target machine evidenced some steps taken to conceal the detection of the continued access | * Continued access to the target machine evidenced excellent steps taken to fully conceal the detection of the continued access |
| Proxy set up 25% | * No evidence of proxy set up | * Proxy set up is evidenced but unsuccessful | * Proxy successfully set up and evidenced no attempt to conceal the detection of the proxy | * Proxy successfully set up and evidenced, but some steps taken are likely to be detectable | * Proxy successfully set up and evidence appropriate steps taken to conceal detection of proxy within the browser | * 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 |
| Self-Assessment is a requirement of this assessment and can be completed on <https://safe.southwales.ac.uk> after the submission date.  After the lecturer has completed assessment you will be given a provisional mark only: subject to change and/or confirmation by the Assessment Board | | | | | | |

# 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. You must first figure out his IP address.

Once you have completed your investigation, you must write a short 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. This report should be no longer than 1000 words.

## Hints:

You may find the following useful:

* Use a tool such as Nmap for the initial scan and detect the IP address in use (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)
  + Enhanced password recovery abilities will gain additional marks. It should be capable of more than just a standard dictionary attack.
  + Comments are a requirement
* 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 MUST include the following:

1. Submit a preliminary report on Price's machine, providing details such as IP address, Operating System, Ports etc
2. Password Recovery
   1. A python script used to attack the computer, along with screen shots showing that Prices machine has been successfully accessed
   2. A copy of the entire /var/log/auth.log file from Price's machine straight after cracking the password. You can use scp or SmarTTY to transfer it.
3. A copy of the entire file: /etc/passwd on Price's machine. You can use scp or SmarTTY to transfer it.
4. Evidence that you have set up a proxy to monitor traffic from Price's machine:
   1. Screenshots of the **ip a** output for both machines (clearly labelled)
   2. Wireshark \*.pcap file from the client external adapter (NAT connector)

Submit all documents to UniLearn.

1. University Academic Misconduct Regulations [↑](#footnote-ref-1)
2. Information on exclusions to this rule is available from the Advice Centre at each Campus [↑](#footnote-ref-2)