

Coursework Specification

# **CW\_Specification\_CSI\_6\_SCS\_2324\_2022/23**

Read this coursework specification carefully, it tells you how you are going to be assessed, how to submit your coursework on-time and how (and when) you’ll receive your marks and feedback.

|  |  |
| --- | --- |
| **Module Code** | CSI\_6\_SCS\_2324 |
| **Module Title** | Systems and Cyber Security |
| **Lecturer** | George Bamfo, Jiaqiu Wang |
| **% of Module Mark** | 60% |
| **Distributed** | **13th March, 2024** |
| **Submission Method** | Submit online via this Module’s Moodle site |
| **Submission Deadline** | **15th April,2024 5pm** |
| **Release of**  **Feedback & Marks** | Feedback and provisional marks will be available in the Gradebook and Turnitin (Rubric) on Moodle within 2-3 weeks from the submission+ deadline. |

Coursework Aim:

This coursework requires the students to undertake an individual project, and work on a real-world cyber-security case study where they will try to perform a traditional black-box penetration testing on a target system.

The students must choose a target from the suggested resources, perform a penetration testing that will include a security assessment (e.g. vulnerability scanning), and submit a professional report. This assessment will be evaluated based on the final report and must be organized into corresponding sections of the given template format, which follows of the Pentest methodology introduced in the class.

The target machine must be selected from the in-scope list given in the “Assessment Task” section.

This coursework will test the students on their knowledge and understanding of cybersecurity and managing and mitigating risks and threats and will allow them to demonstrate these skills in a practical test case.

(See Assignment Task, below).

Coursework Details:

|  |  |
| --- | --- |
| **Type:** | Project Report |
| **Word Count:** | A minimum of 2500 words is recommended with 5000 words maximum limit.  The following texts will be excluded from the word counts.   * Footnotes for reference purpose only. * Bibliography. * List of tables, Figures and Table of Contents. * Source code and scripts. * Everything that is included in the Appendix section.   You might append source codes, development environments, and any additional resources at the appendix section. However, these will be excluded from the marking scope. Please note in case that you develop you own tool or code; the complete source code must be submitted as a separate script for evaluation and correctness as supporting materials. |
| **Document Structure and Readability:** | * The document **MUST** follow the format of the *given template (*[*CW\_Report\_ID.doc*](https://vle.lsbu.ac.uk/mod/resource/view.php?id=1953971) *on VLE)*. * The report must be divided appropriately into sections with the several stages of the pentest methodology introduced in the class. * Work must be cited through appropriate bibliography. * Work must be submitted as a Word document   (.doc/docx) or a PDF (not exceeding 100MB).   * Coursework document must follow a consistenttemplate, using a single font and font size (e.g., Arial 11 or larger if you need to for the headings), with a recommended 1.5 line spacing. * Any code analysis or command execution must becomplete and concise with proper commenting to explain the logic, attributes/options/flags, and input parameters. To present the **Source Code** snippets, command execution, bash scripts, or configuration files, you need to use a fixed-width font and clearly readable (no screenshots), recommended Monospaced fonts (Consolas, Courier New, etc.). You might split the code by module and present it through a table (1x1) used as a code-box, that will clearly separate from the narrative. * Your student ID number must appear at the front page of the coursework. Your name must **not** be on the |

|  |  |
| --- | --- |
|  | report. |
| **Screenshots Requirements** | * Each student before starting any penetration testing, need to create a new user in their Kali-Linux\_VM (attacking) machine with their username along with their **last two digits** of their student-ID. The username could be your first-name, your surname or a combination from the first letters of both, for example “georgeb80”. (Example at the end of this document) * The screenshots need to include your user on eachcommand that is being executed in your Kali-Linux machine, unless if the command requires the ‘root’ user and cannot be executed with “sudo”, or if you are logged into the target machine. (Example at the end of this document) * Screenshots must have a captioned, cross-referenced and should be used mostly to provide evidence of:   + Output or results of a program/tool execution (any command that has been executed as an input must be provided also by text).   + Designs, such as Information on the network environment, IP addresses, activity diagrams/flowcharts etc.   + Present a software interface (GUI/CLI), or tools.   + Graphical Analysis may include a representation of the results or similar type of comparative plots.   + Any other relevant evidence that can be used as a proof of concept (e.g., proof.txt), which may include usernames, attacker IP address, target IP address etc.   Note: Screenshots which do not satisfy the abovementioned requirements will not be considered and the report will be penalised accordingly! |
| **Walk-throughs:** | The use of walk-through(s) for target machines it is **allowed**. However, in case that you will follow a walkthrough, be aware of the following guidelines:   You must provide a reference with citation inside the text of the walk-through(s) that has been used and refer to those even in the beginning of the |

|  |  |
| --- | --- |
|  | report (introduction).   * The contribution and your work on the report needs to be clear comparing with the walkthrough(s). * *You* ***cannot*** *copy/paste*  any of the content, screenshots, or any other evidence from the walk-though(s) in your report. You need to write the report based in your own experience and create your own evidence. Otherwise, may be a subject of **plagiarism**. * Walk-through(s) usually do not follow any specific pentest methodology. You need to organize the content of your report into sections based in the penetration testing methodology discussed in the class. * Walk-through(s) start from active attacks (stage 2 or higher). Make sure that you will include Information gathering and other stages that might be missing of the methodology. * ***Be advised*** : Content included into wrong sections will not be considered for marking (e.g. brute force attack in information gathering section). * Walk-through(s) may include several gaps of information they provide, as the authors often consider those information as “known”. You need   to fill-in those gaps in your report. (e.g., how a password has been found)   * Vulnerability scanning is rarely included, authors may directly provide a way(s) to attempt the exploit, by skipping vulnerability scanning, or security assessment in general. Vulnerability analysis and Enumeration stage must be included   in the report, identifying key threats and vulnerabilities that are about to be exploited, along with a reasonable flow of narrative with justifications.   * Do not blindly follow a walk-through, as it may include outdated tools and methods. |
| **Referencing:** | Harvard Referencing should be used, see your [Library Subject Guide](https://libguides.lsbu.ac.uk/subjects/home) for guides and tips on referencing. |

|  |  |
| --- | --- |
|  | The references must include at least two (or more) of following types of sources:   * (Mandatory) A reference with a link of victim machine and its origin, along with the name of the machine (if applicable). * (Mandatory/Optional) References of any walkthrough(s) or guides that has been used. Note, it’s not a must for a walk-through to be used as a resource, however, it is recommended. If a walkthrough has been used, it is a must to use a reference. * (Optional) References of any forums, or links that have been followed, along with access date and title. * (Optional) Books and other resources studied to accomplish this tasks.   Note: Inappropriate reference formats or mixed referencing will be penalised as stated in the assessment rubric’s report structure and readability criteria! |
| **The Content:** | * The final report must document all the steps, commands issued, and console output in the form of a scientific format. * The documentation should be thorough enough that the pentest can be replicated step-by-step by a technically incompetent reader.   Note: Your report should be narrative in style, with human explanation and commentary. A "report" that is merely a collection of screenshots and data dumps will be graded very poorly. |
| **Submission** | Students could submit up to 2 different FILES:   1. (Mandatory) The main report (.doc, .docx, .pdf), which includes the documentation of the coursework in a scientific format. 2. (Optional) A compressed file (.zip), with the supporting materials e.g., source code or scripts that has been developed (.sh, .py, .cpp, .java), tool release versions (executable file .pyc, .exe, .out, .jar etc.) that are not included into the default Kali-Linux |

|  |  |
| --- | --- |
|  | installation, references/links with code snippets that has been used, dependencies (e.g.  libraries/directives), or other kind of software that is required to recreate the testing environment etc. In case the file size exceeds 100MB, a cloud storage should be used (OneDrive, Google drive, etc.) with appropriate access rights, and submit a single text file (.txt) that will include the link.  Note: Any submission with inaccessible material(s) will not be considered for marking.  The filenames need to have the format:   1. studentID\_name-coursework2\_report.doc (example: 123456\_John\_Doe-coursework2\_report.doc) 2. studentID\_name-project\_materials.zip (example:   123456\_John\_Doe-project\_materials.zip) |
| **Regulations:** | Make sure you understand the [University Regulations](http://www.lsbu.ac.uk/__data/assets/pdf_file/0008/84347/academic-regulations.pdf) on expected academic practice and **academic misconduct**.  **Note in particular:**   * Your work must be your own. Markers will be attentive to both the plausibility of the sources provided as well as the consistency and approach to   the writing of the work. Simply, if you do the research and reading, and then write it up on your own, giving the reference to sources, you will approach the work in the appropriate way and will cause not give markers reason to question the authenticity of the work.   * All quotations must be credited and properly referenced. Paraphrasing is still regarded as plagiarism if you fail to acknowledge the source for the ideas being expressed.   **TURNITIN:** When you upload your work to the Moodle site, it will be checked by anti-plagiarism software. Your similarity index for the report must not be more than 20%. Any report with exceeding a 20% similarity index will be subject to Academic Misconduct Investigation (AMI). |

# Learning Outcomes

This coursework will fully or partially assess the following learning outcomes for this module.

* Develop the in-depth knowledge necessary for enhancing security in modern networks, protocols, and systems.
* Have a solid understanding of the information security technologies.
* Analysis and problem-solving ability through experimentation and testing, with appropriate software solutions and environment setup.
* Acquire in-depth understanding of various cyber security tools.
* Creation of a personal toolset for penetration testing.
* Synthesize and utilize resources/tools by providing an appropriate Cyber-Security technique to solve the given tasks.
* Be able to evaluate and assess the security of a computer system, by conducting a security assessment.
* Evaluate vulnerabilities and security risks, by attempting a vulnerability scanning followed by exploitation techniques to identify false positive and false negative vulnerabilities, and know-how to assess them.
* Analyse systems for security weaknesses and propose mitigating measures to improve the overall security.
* Raise awareness of the risks that are present, identifying assets, and build risk management knowledge to manage and mitigate cyber security threats and vulnerabilities.
* Demonstrate a systematic understanding of Cyber Security awareness based on practical experience of penetration testing.

# Assessment Task

A traditional penetration test has become more commonly used for regularly test security systems and processes and maintain a policy that addresses information security for all personnel. In this category of assessments, security analysts have to go beyond the minimum-security requirements that are designed to actually improve the overall security of the system.

For this purpose, each student is assigned **ONE** target machine that must be compromised. The target machine a student will work on depends on the Group Number. There is an allocation for each student. This can be seen in the excel sheet on [Teams](https://stulsbuac.sharepoint.com/:f:/r/sites/CSI_6_SCSSystemsandCyberSecurity23_24/Shared%20Documents/General/Coursework-VM?csf=1&web=1&e=QP1efg).

The objective is to exploit one target machine and provide proof of exploitation. Stimulate, what would happen if an internal user is compromised, or identify what would happen if the system under testing is subject to an attack by a malicious external party. To achieve that you must complete the following tasks:

* Perform a passive attack gathering information.
* Perform Network discovery on the target network.
* Conduct a Port scanning on the target, documenting service that are running, protocols, application version, identify operating system etc.
* Conduct a vulnerability scanning, analysing the results and identify the risks.
* Leverage identified issues to uncover the worst-case scenario.
* Follow up with validation of the findings through the use of exploits or tests to eliminate false positives and detect hidden vulnerabilities or false negatives. This involves exploiting the vulnerabilities discovered.
* Explore the level of access each exploit provides and use increased access as leverage for additional attacks. Some of the machines may require multiple exploitation steps, resulting first in low-level local access, and then in root or administrative as vertical privilege escalation.
* If none of the exploits are successful, a Denial-of-Service attack could be attempted.

The final goal is to gain access into a file called “proof.txt” located in user root home directory on most of the target machines. In case that this file does not exist, make sure that you provide other kind of evidence of root access, that clearly shows the access level that has been achieved.

Attempts to perform Pilfering, Tracks Covering and Backdoor Creation are optional and could be considered as bonus that cannot exceed the 10% of the coursework.

This assessment will be evaluated based on the final report and must be organized into corresponding sections of the given template format. This template follows the Pentest methodology introduced in the class. For more details on each stage of the penetrations testing methodology, refer on Week-5 and course materials on VLE.

# Assessment Criteria and Weighting

The report will be marked using the marking criteria provided in this coursework specification document. All the students are advised to fully understand the marking criteria before starting the coursework.

LSBU marking criteria have been developed to help tutors give you clear and helpful feedback on your work. They will be applied to your work to help you understand what you have accomplished, how any mark given was arrived at, and how you can improve your work in future.

**Marking Criteria**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Criteria** |  | **Feedforward comments** |  |  |  |  |
| **Weighting** | **Excellent (100-71%)** | **Good**  **(70-61%)** | **Pass**  **(60-51%)** | **Weak**  **(50-41%)** | **Poor**  **(40-0%)** |
|  | **Report and Documentation** | |  |  |  |  |  |
|  | **Report Structure and**  **Readability**  **(Marks 10%)** | 10% | Sophisticated, consistent, error free application of relevant topics conventions with great attention to detail.  Excellent writing, structure, spelling, grammar. | Comprehensive application of relevant topics conventions with few errors.  Very good writing, structure, spelling, grammar, but with minor errors. | Generally correct application of relevant topics conventions, with some errors and / or inconsistencies. The length of the report is at least 2500 words.  Sufficiently written with little structure, spelling, grammar with some errors. | Poorly written with confusing structure, spelling, grammar and / or errors. Below the minimum of 2500 words. | Poorly written, less than 2500 words, with no academic style, structure, spelling, grammar and/or multiple errors.. |
|  | **Introduction**  **(Marks 5%)** | 5% | A well-articulated introduction that provides a clear, logical, and succinct description of content, objectives, scope, and requirements. The organization of the review, which draws the reader’s attention to a central concern, debate, or contention. | A well-articulated introduction that provides a clear, logical description of content, objectives, scope,  requirements, and organization of the review | An introduction that describes the content, objective, scope, and organization of the report. | An introduction that outlines the content, scope, and organization of the report | Either no introduction or one that poorly or partially situates the reader in the context of the concern, debate, or contention addressed in the report |
|  | **Summary and**  **Recommendations**  **(Marks 5%)** | 5% | Excellent breadth, accuracy, and detail in understanding key aspects of subject. Contributes to subject debate. Very good awareness of ambiguities and limitations of knowledge.  Provides high-level summary and recommendations are very accurate and detailed | Good depth of understanding of key aspects of subject shown Evidence of coherent knowledge. Very good contribution to subject debate.  Very good summary and accurate recommendations | Demonstrated good understanding of key aspects of subject. Some evidence of coherent knowledge and own critique.  Sufficiently summarize the report with some recommendations | Weak evidence of superficial understanding of subject. Inaccuracies.  Some outline of  recommendations, does not summarize well the report or lack of succinctness. | Little or no evidence of understanding of subject. Inaccuracies.  Without any recommendation, does not summarize the report. |
|  | **Methodology** | |  |  |  |  |  |
|  | **Information Gathering**  **(Marks 10%)** | 10% | Excellent problem-solving ability and implementation of the proposed methodologies and solutions.  Ability to Adapt to unforeseen practical and theoretical challenges to achieve project objectives. Well-crafted technical solution, addressing all aspects of the user requirements. | Very good problem-solving ability and implementation of the proposed methodologies and Solutions.  Adapt to practical and theoretical challenges to achieve project objectives. Comprehensive technical solution, addressing various aspects of the user requirements. | Sufficient problemsolving ability and implementation of the proposed methodologies and solutions.  Some adaptation to practical and theoretical challenges to achieve project objectives identified goals. Good technical solution, addressing most aspects of the user requirements. | Limited problem-solving ability and implementation of the proposed methodologies and Solutions.  Limited exploration of possible solution(s) using established approaches to resolve practical and theoretical problems. Weak attempt at the technical solution, addressing only few aspects of the user requirements. | Poor or lack of problem-solving ability and  implementation of the proposed methodologies and solutions.  Little or no exploration of solution(s). Question or problem unresolved. Poor attempt at technical proposition. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Scanning and Mapping**  **(Marks 15%)** | 15% | Excellent problem-solving ability and implementation of the proposed methodologies and solutions.  Ability to Adapt to unforeseen practical and theoretical challenges to achieve project objectives. Well-crafted technical solution, addressing all aspects of the user requirements. | Very good problem-solving ability and implementation of the proposed methodologies and Solutions.  Adapt to practical and theoretical challenges to achieve project objectives. Comprehensive technical solution, addressing various aspects of the user requirements. | Sufficient problemsolving ability and implementation of the proposed methodologies and solutions.  Some adaptation to practical and theoretical challenges to achieve project objectives identified goals. Good technical solution, addressing most aspects of the user requirements. | Limited problem-solving ability and implementation of the proposed methodologies and Solutions.  Limited exploration of possible solution(s) using established approaches to resolve practical and theoretical problems. Weak attempt at the technical solution, addressing only few aspects of the user requirements. | Poor or lack of problem-solving ability and  implementation of the proposed methodologies and solutions.  Little or no exploration of solution(s). Question or problem unresolved. Poor attempt at technical proposition. |
|  | **Enumeration**  **(Marks 15%)** | 15% | Excellent problem-solving ability and implementation of the proposed methodologies and solutions.  Ability to Adapt to unforeseen practical and theoretical challenges to achieve project objectives. Well crafted technical solution, addressing all aspects of the user requirements. | Very good problem-solving ability and implementation of the proposed methodologies and Solutions.  Adapt to practical and theoretical challenges to achieve project objectives. Comprehensive technical solution, addressing various aspects of the user requirements. | Sufficient problemsolving ability and implementation of the proposed methodologies and solutions.  Some adaptation to practical and theoretical challenges to achieve project objectives identified goals. Good technical solution, addressing most aspects of the user requirements. | Limited problem-solving ability and implementation of the proposed methodologies and Solutions.  Limited exploration of possible solution(s) using established approaches to resolve practical and theoretical problems. Weak attempt at the technical solution, addressing only few aspects of the user requirements. | Poor or lack of problem-solving ability and  implementation of the proposed methodologies and solutions.  Little or no exploration of solution(s). Question or problem unresolved. Poor attempt at technical proposition. |
|  | **Gaining Access**  **(Marks 25%)** | 25% | Excellent problem-solving ability and implementation of the proposed methodologies and solutions.  Ability to Adapt to unforeseen practical and theoretical challenges to achieve project objectives. Well crafted technical solution, addressing all aspects of the user requirements. | Very good problem-solving ability and implementation of the proposed methodologies and Solutions.  Adapt to practical and theoretical challenges to achieve project objectives. Comprehensive technical solution, addressing various aspects of the user requirements. | Sufficient problemsolving ability and implementation of the proposed methodologies and solutions.  Some adaptation to practical and theoretical challenges to achieve project objectives identified goals. Good technical solution, addressing most aspects of the user requirements. | Limited problem-solving ability and implementation of the proposed methodologies and Solutions.  Limited exploration of possible solution(s) using established approaches to resolve practical and theoretical problems. Weak attempt at the technical solution, addressing only few aspects of the user requirements. | Poor or lack of problem-solving ability and  implementation of the proposed methodologies and solutions.  Little or no exploration of solution(s). Question or problem unresolved. Poor attempt at technical proposition. |
|  | **Escalating Privileges or**  **Denial of Service**  **(Marks 15%)** | 15% | Excellent problem-solving ability and implementation of the proposed methodologies and solutions.  Ability to Adapt to unforeseen practical and theoretical challenges to achieve project objectives. Well crafted technical solution, addressing all aspects of the user requirements. | Very good problem-solving ability and implementation of the proposed methodologies and Solutions.  Adapt to practical and theoretical challenges to achieve project objectives. Comprehensive technical solution, addressing various aspects of the user requirements. | Sufficient problemsolving ability and implementation of the proposed methodologies and solutions.  Some adaptation to practical and theoretical challenges to achieve project objectives identified goals. Good technical solution, addressing most aspects of the user requirements. | Limited problem-solving ability and implementation of the proposed methodologies and Solutions.  Limited exploration of possible solution(s) using established approaches to resolve practical and theoretical problems. Weak attempt at the technical solution, addressing only few aspects of the user requirements. | Poor or lack of problem-solving ability and  implementation of the proposed methodologies and solutions.  Little or no exploration of solution(s). Question or problem unresolved. Poor attempt at technical proposition. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Bonus** |  |  |  |  |  |  |
|  | **Pilfering, Tracks**  **Covering, Backdoor Creation**  **(Bonus Marks 10%)** | 10% | Excellent problem-solving ability and implementation of the proposed methodologies and solutions.  Ability to Adapt to unforeseen practical and theoretical challenges to achieve project objectives. Well crafted technical solution, addressing all aspects of the user requirements. | Very good problem-solving ability and implementation of the proposed methodologies and Solutions.  Adapt to practical and theoretical challenges to achieve project objectives. Comprehensive technical solution, addressing various aspects of the user requirements. | Sufficient problemsolving ability and implementation of the proposed methodologies and solutions.  Some adaptation to practical and theoretical challenges to achieve project objectives identified goals. Good technical solution, addressing most aspects of the user requirements. | Limited problem-solving ability and implementation of the proposed methodologies and Solutions.  Limited exploration of possible solution(s) using established approaches to resolve practical and theoretical problems. Weak attempt at the technical solution, addressing only few aspects of the user requirements. | Poor or lack of problem-solving ability and  implementation of the proposed methodologies and solutions.  Little or no exploration of solution(s). Question or problem unresolved. Poor attempt at technical proposition. |

# How to get help

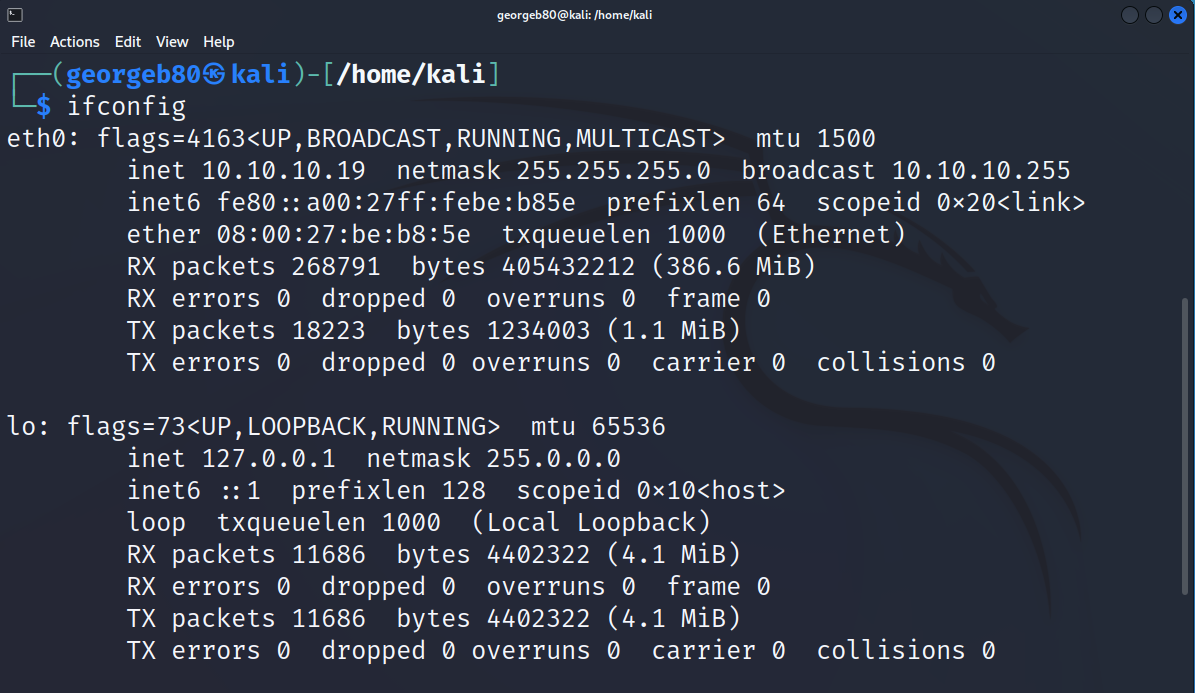
We will discuss this Coursework Specification in class. However, if you have any related questions, please feel free to contact the Module Leader on MSTeams or via email at bamfog3@lsbu.ac.uk as soon as possible.

# Screenshot Requirements Example

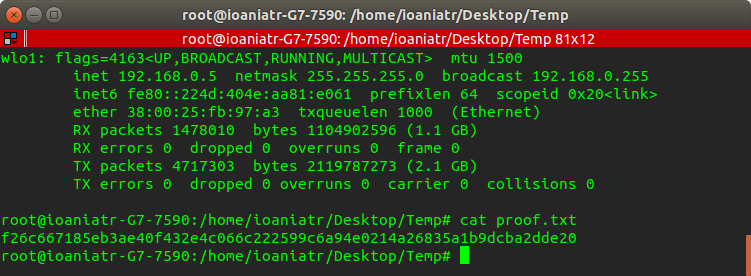
The commands to add a new user in a Linux machine are the following:

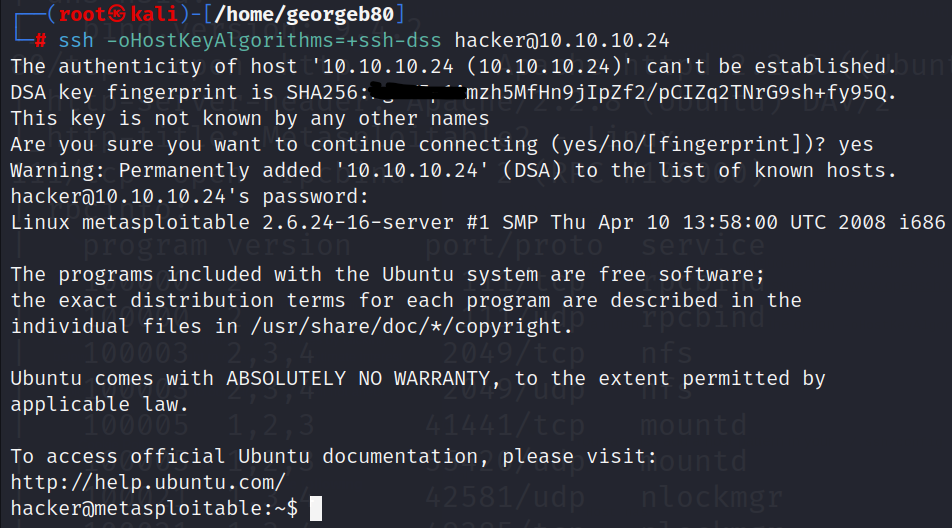
|  |
| --- |
| root@kali:~# useradd -s /bin/bash -m georgeb80  root@kali:~# usedmod -aG sudo georgeb80  root@kali:~# passwd georgeb80  New password: Retype new password:  passwd: password updated successfully  root@kali:~# su georgeb80 georgeb80@kali:~$ |

Clearly show the IP address of your machine that you are making the attack by using ‘*ifconfig*’, for example:



As a proof of concept, for each ‘*proof.txt*’ or any other evidence found must be shown in a screenshot that includes the entire contents of the file, along with the IP address of the target by using “*ifconfig*” or “*ipconfig*”. For example:





This way we make sure to include screenshots as evidence for proof of concept that include at least the following information:

* The student username after executing CLI command.
* The remote system user in the attacker’s machine.
* Attacker IP address  Target IP address

# Resources

All the module’s lectures, tutorial handouts, and references are recommended in the module guide. Some links that may be found useful:

Kali-Linux Tools list: [Link](https://www.kali.org/tools/)

Kali-Linux Revealed (Online free course): [Link](https://portal.offensive-security.com/courses/pen-103/books-and-videos/modules)

Nmap Reference Guide: [Link](https://nmap.org/book/man.html)

Nessus Documentation (by Tenable): [Link](https://docs.tenable.com/Nessus.htm)

OpenVas Guide: [Link](https://hackertarget.com/openvas-tutorial-tips/)

Metasploit Unleased (Online free course): [Link](https://www.offensive-security.com/metasploit-unleashed/)

Exploit-DB (by Offensive-Security): [Link](https://www.exploit-db.com/)

JohnTheReaper Cheat Sheet: [Link](https://countuponsecurity.files.wordpress.com/2016/09/jtr-cheat-sheet.pdf)  HashCat Guide: [Link](https://hashcat.net/wiki/doku.php?id=hashcat)

Highly recommended books from the reading list:

* Hacking Exposed 7: network security secrets & solutions (ISBN: 978-007-178029-2)
* CEH v9 (ISBN: 978-1-119-25224-5)

To learn more on how to access research E-resources and publications. Please visit:

[https://library.lsbu.ac.uk/friendly.php?s=LSBU-Library-and-LearningResources/Home](https://library.lsbu.ac.uk/friendly.php?s=LSBU-Library-and-Learning-Resources/Home)

# Quality assurance of coursework specifications

Coursework specifications within CSI division go through internal (for new modules with 100% coursework also through external) moderation. This is to ensure high quality, consistency and appropriateness of the coursework as well as to share best practice within the CSI division.