Info3002 Ethical Hacking Principles and Practice

Pentesting Project

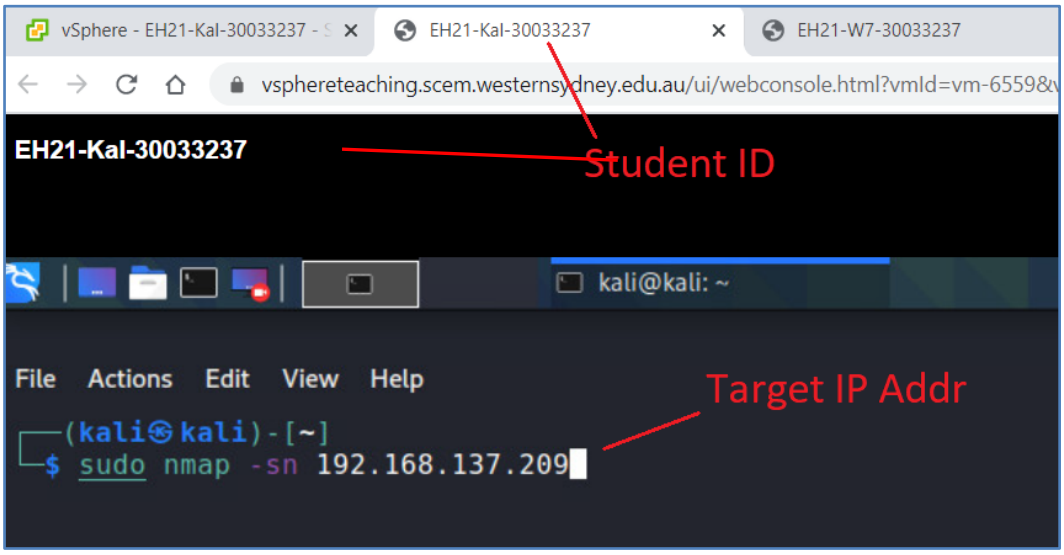
Due: 9pm, Friday, 9 June 2023

This project is of individual work. Any collaboration with others and any use of Generative AI tools are prohibited.

In this project, you will pentest the Metasploitable2 VM and play picoCTF (the Capture The Flag challenges from Carnegie Mellon University).

Since pentesting is of exploration nature, you should try to complete the tasks without asking tutors any questions. There are hints and notes provided within this document to help you. Besides these, you should do research yourself first if you encounter difficulty in completing a task. For instance, if you do not know the usage of the '*xxx*' command and its options, use 'man *xxx*' to find out. After you have tried almost everything and still cannot figure out, limited help can be obtained from tutors.

Write your answers for all tasks into a project report. When asked to grab a screenshot in a task, the screenshot must include the VM name which includes your **Student ID**. If you are using VMs created on your own laptop, then the screenshot must show the IP address of the target somewhere. For instance, the target IP can appear in your command line, or if the command line does not include the target IP, you can use 'ip a' command to display the IP address intentionally. An exemplar screenshot is included as follows. Failing to do so will cause you lose marks for relevant tasks.



You are suggested to read the entire specification first, and then start with the tasks that are already covered by our lectures. Especially, you should start to work on Task 5 (picoCTF) as early as possible.

1 Service and Vulnerability Detection [3 marks]

1.1 If using nmap to scan all TCP ports of Metasploitable2 instead of the default 1000 ports, it will show that the port 8787 is open. Suppose you are interested in knowing which service is running on this TCP port. Use nmap to scan only this port to achieve this. [1 mark]

a) Include a screenshot showing your command line and its output.

b) Then, based on the output, use your own words to describe the detected service and software version into your report.

1.2 In GVM, explore its interface to create a port list with all TCP ports 1-65535 included (let's ignore port 0, which is a port number not supported by all OS kernels). Name this port list **All TCP Ports**. Then, create a target for scanning the Metasploitable2 VM with this port list. Finally, create a task to scan this target with 'Full and Fast' as the Scan Config.

a) Detail your steps for achieving the above into your project report and include a screenshot for port list creation, target creation and task creation respectively. [1 mark]

b) Complete the scan task created above, and obtain the PDF report from this scan. Compare this report (denoted by **Report 1**) with the report you obtained from Lab 4 Task 4.8 (denoted by **Report 2**). Detail how you have made the comparison, and give at least one TCP port that is shown to have severity 'High' results in **Report 1**, but not listed in **Report 2**. Also, list the severity 'High' results from that port. [1 mark]

2 Exploitation [3 marks]

2.1 The "Metasploitable 2 Exploitability Guide" (https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide) gives a great tutorial on how to exploit the Metasploitable2 VM. Please read through this guide, and especially focus on the 'Services: Backdoors' section. Then, accomplish the following tasks.

a) The 'Services: Backdoors' section first describes how to manually exploit the backdoor in the tampered FTP server VSFTPD v2.3.4. Follow it to complete the exploitation on your Metasploitable2 using 'nc' instead of 'telnet'. Detail your steps and include a screenshot on your success. This screenshot should include the 'nc' command line, and the results of executing the following commands after gaining access: 'id', 'ip addr show dev eth0', and 'hostname'.

[1 mark]

Note: The 'telnet' command has been deprecated in Linux today. This is why you are asked to use the 'nc' command instead. The 'nc' command runs the 'netcat' tool, which is very flexible and is dubbed 'the Swiss army knife for networking'. The 'netcat' tool will be covered in Week 7's lecture.

b) The 'Services: Backdoors' section also describes how to exploit the old standby "ingreslock" backdoor that is listening on port 1524. Use the 'netcat' tool instead of 'telnet' to accomplish this exploitation. Detail your steps and include a screenshot on your success. This screenshot should include the 'netcat' command line, and the results of executing the following commands after gaining access: 'whoami', 'ip a show dev eth0', and 'pwd'. [1 mark]

2.2 Your GVM report for Metasploitable2 obtained in Task 1.2 should show the 'distcc Remote Code Execution Vulnerability' on TCP port 3632. Follow the Section 6 Steps 1-5 from the following tutorial

https://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson2/index.html to exploit this vuln. Detail your steps and include a screenshot on your success. This screenshot should include the results of executing the following commands after gaining access: whoami and 'ip a show dev eth0'. [1 mark]

Note: The 'BackTrack' mentioned in this tutorial is the previous name of Kali Linux. Moreover, since Kali 2020, you need to add 'sudo' before 'msfconsole' when starting msfconsole.

3 Post Exploitation [3 marks]

After completing Task 2.2, you will notice that the user account you get is 'daemon', not 'root'. Follow the Section 6 Steps 6-10 from the tutorial mentioned in Task 2.2 to escalate the privilege to 'root'. Detail your steps and include a screenshot on your success. This screenshot should include the results of executing the following commands in the obtained 'netcat' session: 'whoami' and 'ip a show dev eth0'. The different things you should do from this tutorial are mentioned in the hints below.

[3 marks]

Hints:

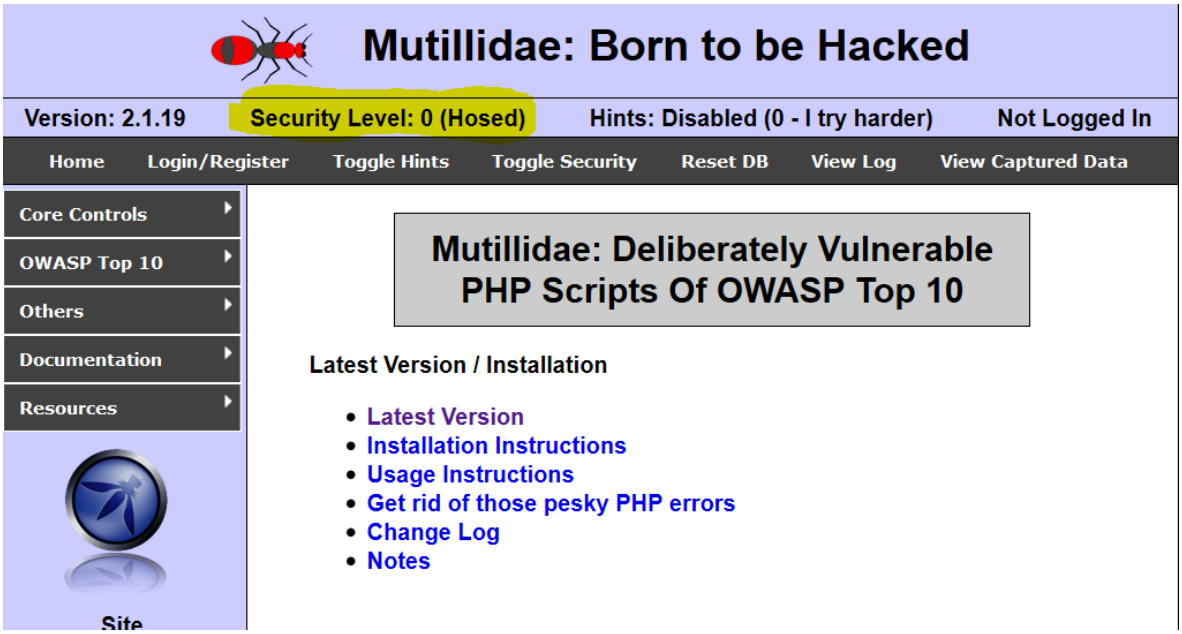
- In case the VMs in our school cloud are not allowed to visit exploit-db.com (due to uni firewall rules), you can obtain the 'exploit-8572.c' through another method. For example, you can use 'searchsploit' to find it in the local installation of exploit-db in your Kali. You will see that it is named '8572.c' in the local installation of exploit-db. Refer to our lecture 5 about 'searchsploit'.
- To upload '8572.c' to Metasploitable2, there can be several methods. Here we suggest to you to use netcat, which is available in both Metasploitable2 and Kali. Basically, in your Kali, start a new terminal, and then run 'netcat' in server mode to transfer this file, and finally hit 'Ctrl +c' to end the transmission when you estimate the transmission is over. And in the remote shell you obtained in Task 2.2, run 'netcat' in client mode to receive this file; after the transmission is over, use 'ls -l' to double check if it is received.
- In Linux, sometimes you don't see responses to your commands, but you should still proceed. Check if it is a success by issuing verifying command.
- Since Kali 2020, 'sudo' is needed when running 'netcat' in server mode.

This task is challenging. Be careful and make sure you understand every step. You can also watch the following video on Youtube to get a clearer idea on this privilege escalation: https://www.youtube.com/watch?v=DoUZFHwZntY .

4 Web Pentesting [4 marks]

In our lectures and labs, we used the DVWA as our web pentesting target. In this project, you will be asked to pentest another intentionally vulnerable web application called 'Mutilliadae', which is also installed in Metasploitable2.

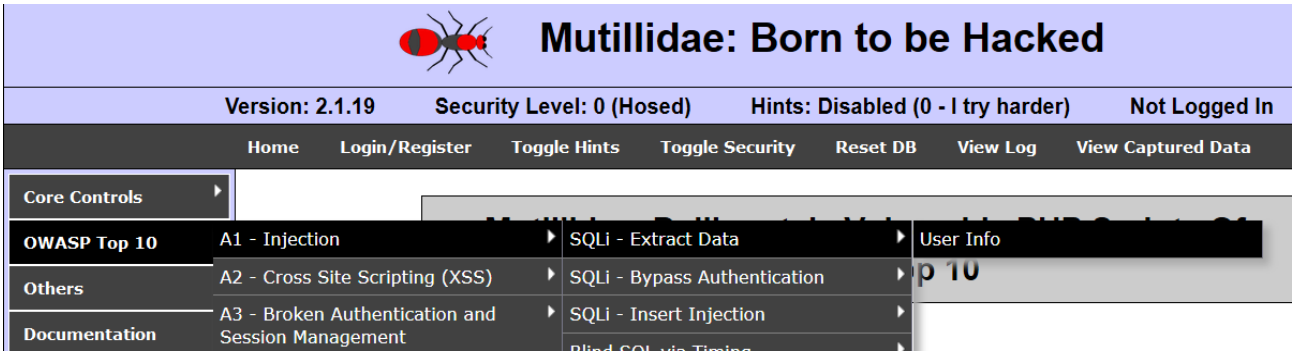
The use of Mutillidae is straightforward. Simply enter the following URL into Firefox: http://<IP of Metasploitable2>/mutillidae/, and you will see the Mutillidae interface. If you see there are warning messages from the database, you should click the 'Reset DB' link in the Mutillidae interface to restore the database to its initial state. Then, those warning messages should disappear. Note that, different from DVWA, you do not need to log into Mutillidae to access its pages. Also note that, the default security level of Mutillidae is '0' (the lowest security level) when you start browsing this application (see the screenshot below). This is the security level you should use during your pentest, and you should leave it as it is, i.e., never toggle it.



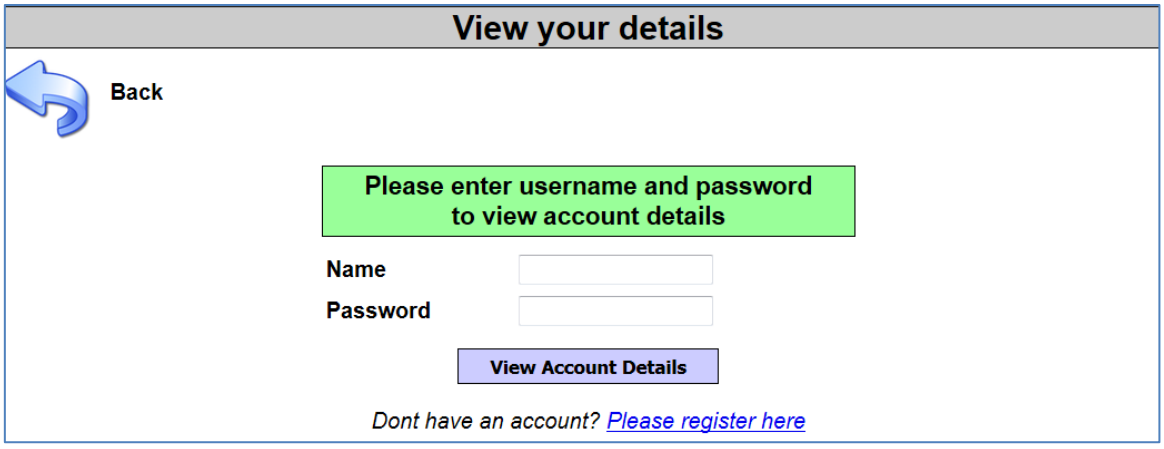
Mutillidae contains the pages corresponding to the OWASP Top 10 Security Risks. These pages can be accessed by the 'OWASP Top 10' menu located in the left. In this project, you are only required to pentest the SQLI page and the Stored XSS page among them. The detailed instructions are given below.

4.1 The SQLI page. [2 marks]

Click 'OWASP Top 10' → 'A1 – Injection' → 'SQLi – Extract Data' → 'User Info' as shown below.



You will reach the 'user-info.php' page as shown below:



In this page, enter crafted inputs for 'Name' and 'Password' respectively, such that the details of all users stored in the database are displayed. You should:

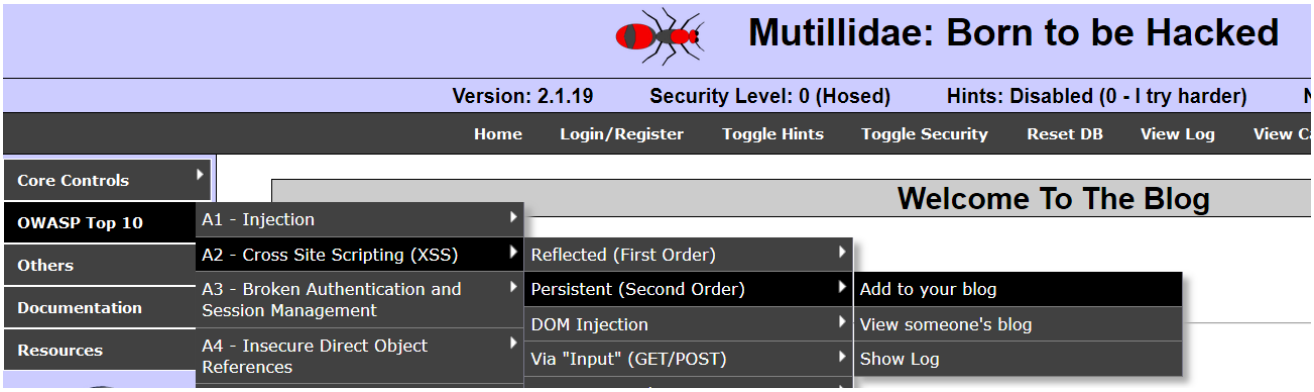
a) Write your crafted inputs into the project report.

b) Also, include a screenshot to prove your success (showing the details of at least three users).

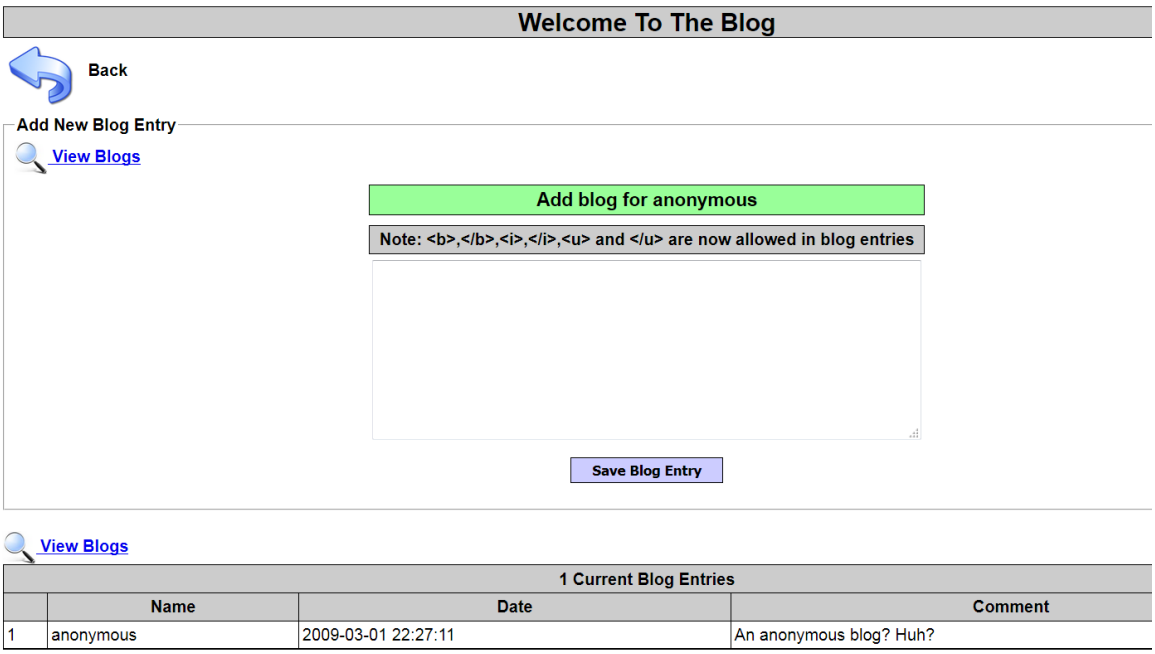
Hint: you can try the valid inputs (Name: admin, Password: adminpass) first.

4.2 The Stored XSS page. [2 marks]

Click 'OWASP Top 10' → 'A2 - Cross Site Scripting(XSS)' → 'Persistent(Second Order)' → 'Add to your blog':



You will reach the 'add-to-your-blog.php' page as shown below:



In this page, enter a crafted blog entry which can report the cookies of a web session to a server you set up. You should then use another browser to view this blog entry, and have the cookie for this new browsing session reported to the server you set up. This another browser can be the IE on Win7 VM. If you set up your own lab environment, you should make sure to have a third VM in it, such that you can use the browser on the third VM to browse your crafted blog entry.

You can follow the Lecture on Cookie and XSS to achieve the above. In your project report, you should include the following:

a) Detail your steps of setting things up such that when another browser visits your crafted blog entry, the cookie of this browsing session will be disclosed to you.

b) Your crafted blog entry.

c) A screenshot on the received cookies by the server you set up.

5 Playing picoCTF [7 marks]

CTF (Capture The Flag) is a kind of cyber security competition in which contestants submit flags to prove that they have solved a challenge. A flag is a secretive string that is found out after solving a challenge.

There are many CTF competitions held around the world every year. Among these CTFs, picoCTF (https://picoctf.com/) is one of the most famous. It is developed by the security experts at Carnegie Mellon University mainly for high school students. However, due to its profound technical depth, it is widely participated by university students as well.

The picoCTF has been held annually since 2018. Although the past events were over, the challenges in them have been made available for playing at your own pace in the picoGym on the picoCTF website. In this task, you will be asked to play the challenges in picoGym. You can pick any challenges. The detailed instructions are as follows.

1. Visit https://play.picoctf.org/ to register an account. Your username must be in the format of '**wsu**' concatenated with **your student id**, e.g., **wsu19974196**. Since our university email system blocks the emails from picoctf.org (which is true last year), you should use your personal email address for this registration. The website will send you a link to your email address for verification. Note that this email may go to your Junk/Spam folder.
2. After registering successfully, click the 'Classrooms' link on the top of the website to join our Classroom using the Invite Code: "`CKgiZNpRt`". Our classroom is named '`EHPP-2023`'. Your joining request will be sent to us for approval. We'll do the approval on a weekly basis, so please allow one week for your request to be approved. Even when your classroom status is pending, you can still play in the picoGym.

   NB: The joining of our classroom is a must, since it allows us to verify your score. **If you don't join our classroom, you'll receive 0 mark for this task.**
3. Click the 'Practice' link on the top of the website to play in the picoGym. The gym contains many categories of challenges, e.g., 'General Skills', 'Binary Exploitation', 'Cryptography', 'Web Exploitation', etc. It also organizes these challenges according to where they are originally from, e.g., picoctf 2021, picoctf 2022, etc. You can attempt challenges from any category and from any event. Initially, the displayed challenges have small point values. However, while you make progress, the point values of the challenges will become larger and larger.
4. The solutions to many challenges in picoGym can be found on the Internet. You are not recommended to look at those solutions. However, if you still cannot figure out after trying hard, you are allowed to look at them.
5. **Do not submit the flags from others**, **since the flag of a challenge is made different from user to user**. If you submit the flag from another user, the system will surely detect that and report your plagiarism into our classroom. Below is an exemplar screenshot of such plagiarism reporting (with username removed):

Suspicious Submissions

Problem Name	Flag	Date
So Meta	picoCTF{s0_m3ta_505fdd8b}	Tue May 12 2020 13:53:01 GMT+1000 (Australian Eastern Standard Time)

If you are caught with copying flags, you will be punished seriously according to our uni's academic misconduct policy.

6. After submitting the flag of a challenge successfully, you'll receive the points assigned to this challenge from the system. Try to solve as many challenges as you can.
7. In your project report, include your **username** and **score** at picoGym. Also, you should detail the solutions to some selected challenges (which challenge to select is at your discretion). The total points of these selected challenges should be at least 500. The solutions for all challenges are not needed. We will verify your score from our classroom.
8. **Marks calculation:** This task is worth 7 marks. Your marks are based on your picoGym score as follows:

<200	>=200	>=500	>=1000	>=2000	>=3000	>=4000	>=5000
0	1	2	3	4	5	6	7

Note: If you want to check your previously submitted flags, please visit your 'Account Settings' at picoCTF website. Then, click the 'Download Account Data' link. You'll receive the data via your registered email address. In the data, the 'submissions.json' file contains your submitted flags. The 'feedback.json' will tell you if any plagiarism has been detected. If it doesn't contain the phrase 'suspicious submission', then no plagiarism is detected.

Report submission

- Your report should be in PDF format. Name your report Surname-StudentID.pdf.
- Submit to turnitin via the Project Submission link on vUWS. Turnitin will calculate the similarity percentage of your report to other submissions. If you are detected with plagiarism by turnitin, you will be punished seriously according to university policy. Note: To prevent those tricks of bypassing plagiarism detection, we will not show the similarity percentage to you after your submission.
- Make sure you see the confirmation of submission displayed on the screen and double check your submission is there.

Marking Criteria

The mark allocation for each task above is indicated beside it. We will conduct marking with a rubric reflecting this mark allocation. This rubric can be viewed by clicking the pentesting report submission link on vUWS, and then clicking the rubric icon  before the 'Submit' button.

Note that this pentest report has a much higher requirement on writing than lab reports. This is because (1) the writing of pentest reports is of great importance as discussed in our lecture; (2) writing deepens your understanding on techniques; and (3) writing is a key professional skill.

In the rubric, there are three categories of marks for each task: Excellent, Adequate, and Incomplete. The meanings of these three categories are as follows:

- **Excellent (full mark):** The report includes all the command lines and critical screenshots such that another person can exactly repeat what you have done, and both the steps and the results are correct. Moreover, use a narrative style similar to the sample report accompanying the Project Specification on vUWS to describe how you accomplish a task. We will detail the writing of ethical hacking report in Lecture 9. We only require the narrative for each task, and an overall narrative such as executive summary is not required for this report. Your narrative should:
    - Has a label corresponding to its task label such as 1.1, 1.2, 3.1, etc.
    - Be easy to understand. If hard to understand, we will deem your steps incorrect.
    - Use full sentences.
    - Contain no more than one poor instance of the following for each task: typo, grammatical error, non-smooth sentence.
- **Adequate (a mark less than full mark):** The reports include all the command lines and critical screenshots such that another person can easily repeat what you have done, and both the steps and the results are correct. However, the narrative fails to satisfy one of the itemized requirements above for ‘Excellent’.
- **Incomplete (0 mark):** Any critical step or the result is missing or wrong. Note that we’ll be strict with this one. So make sure to include all the command lines and critical screenshots for each task.