A picture containing text, clipart

Description automatically generated

**UNIVERSITY OF HERTFORDSHIRE**

Department of Computer Science

MSc Cyber Security with Advanced Research

7COM1070 – Cyber Security Masters Project

April 2022

**Interim Project Report**

**Name:** Constantin-Alexandru Apetrei

**Student ID:** 14168072

**Supervisor:** Georgios Pissanidis

**Introduction & Overview**

The report provides information of the project research and the practical investigation of the final year project and the technical work that will take place during the investigation process. It will also include an overview of the progress to date and the project plan that will be used to produce a complex project.

The project is about **Penetration Testing the Cloud.** Accoriding to Yurtseven and Bagriyanik, the cloud pen testing is a simulated cyber-attack used against a specific system which is hosted by a Cloud Provider, such as Amazon (AWS) and Microsoft (Azure). In this project the cloud provider will be the Amazon (AWS) and the main objective of the penetration test is to find all the possible weaknesses and to also see how strong the system is; so its security issues can be evaluated. As associated to securing a traditional network infrastructure, the cloud penetration testing can become very complex, challenging, and restrictive. A lot of things will be involved in this project and there will also be a sequence of complex stages that will be used to generate a Penetration Testing report. Pen testing is known as the practice of testing a computer system, network, and any kind of hosted application to find issues that hackers can use for an attack. This type of testing the system is very important as it keeps the security team aware of any danger and also allows them to identify the potential weaknesses that can happen during an attack.

The project will aim to answer the next research question: “How effective does an in-house penetration testing have on the Cloud Environment”? In order for the project to be successful, there will be a lot of things involved to perform the pen test as the tester needs to think and act as a hacker. That is what a penetration tester really is and the target here is to locate any problem associated with the cloud’s security. A plan will be needed to execute a successful penetration test. The best way will be to have an attack and defence setup which will be ready to test automated defence systems while having the chance to discover potential security vulnerabilities. There is a difference between the regular system penetration testing and the cloud penetration testing; the main important one is the cloud provider’s policy. This huge factor can make a cloud pen—test complicated if there is no private cloud.

The design part of the project will involve the cloud penetration testing part where there will be a mixture of internal and external penetration testing techniques which will need to be used to examine the external posture of the cloud environment. The documentation part will be the policy and the authorisation information used to perform the cloud pen-test. A list of steps needs to be taken in order to execute a penetration testing. The first step is to make sure the policies of the cloud provider are known because this could be a risk if the test will be performed without being aware of the specific policies. For example: if you have an application which runs on a public cloud and you decide to attack it then the penetration test will look like a DDoS attack and the cloud provider can shut down your account. The second step is to create a specific pen-testing plan which will be extremely helpful in performing the test; the plan will include the following items: applications, data access, network access, virtualisation, compliance, automation, and approach; this plan will need to be strictly followed. Selecting the right pen-testing tools is also particularly important as there are a lot of tools able to help with the pen-testing process. These tools can simulate a real attack and will help the process to find the specific vulnerabilities of the cloud. The next stage is to observe the response, both human and automated responses are important because there is the part where we can see how the humans and the system responded to the attack. The final step is to formulate a penetration testing report which will include any vulnerabilities, if there are any, and they will need to be reported to the cloud provider to deal with them.

Based on the research performed it is important who is doing the penetration testing. If it is a done in house means that some issues will not be found. This is the main risk of this project as this project will be mostly done in-house. So, the main challenge will be to perform a solid penetration testing and to try to find weaknesses, if there are any. The project will be a challenging one as I have some background knowledge on the penetration testing field as it was a part of my first year in my masters’ degree and the module name was also: penetration testing but this time, the real challenge is to attack the services on the AWS. There are a lot of things to discover and new methods to be learned during the project but this final year project is here to help students to make best use of their skills gained and to also learn new techniques as well. One of the main important factors is that the penetration testing is not only an option. This is the only available option to prove that your cloud environment (e.g., applications) and data are protected enough to allow the highest amount of user access with the lowest amount of risk.

The main purpose of this project will be to determine if these normal or “in-house” penetration testing (pen-tests done by someone who does not work for an organisation) are able to discover any weaknesses that the cloud environment could have, taking in consideration the fact that these penetration tests are free and the cloud providers (AWS in this case) does not pay for it.

**Progress to Date**

The project will consist of several chapters that will help you to understand and to demonstrate how it was designed. The 5 main chapters: Introduction, Literature Review, Methodology, Results & Discussions and Conclusion. They will be used to give an overview of the project aims & objectives, information about the subject, methods on how to plan & execute the pen test and the results that will be discussed in order to answer the RQ.

The main part of the research has been performed where the main aims and objectives have been established. First of all, to perform a penetration testing, a list of phases is need. The following phases have been performed in order to establish the penetration testing aim: the scope has been defined which includes the target systems and the cloud’s services. The next step was to decide what kind of penetration test is needed to be conducted here, such as: white, black, or grey box. A list of expectations was also needed here as this list will be added to the final project report in order to illustrate what was trying to be achieved at this stage and what has been achieved after the penetration test executions. A timeline has also been determined for the technical evaluation part in order to produce correct reports and potential remediation. Another important point that has been performed is the research part of the project which determined the research question. Based on the multiple information obtained from the different papers, articles, and journals the research question has been established which will be tried to be answer based on the practical results and information that will be found.

At the moment the main focus is to create a cloud environment for the test to take place and this will be created using the AWS cloud services such as EC2 instances, RDS, Aurora, API Gateways, Lambada, CloudFront or Lambada Edge functions.

**Consideration of ethical, legal, professional, and social issues**

There is no need for any ethical, legal, or social issues to be taken in consideration as this project will not include people or a form needed to be sent to AWS in order to obtain the permission. Most of the public clouds providers will allow anyone to carry out a penetration testing by respecting and following their strict policy and to let them know before you start the penetration test. Amazon Web Services (AWS) no longer require any authorisation to perform a cloud penetration test for them; the only problem is that AWS might have some exception which needs to be checked by having a look at their policy before performing a pen-test. Thinking about the programs involved in the project this part will be covered by the penetration testing tools and techniques that will be needed to perform this kind of tests. The main way of taking advantage of the AWS policy is to execute a penetration test against a customer and that is why I will use my own account to perform such a test. The exception here is to be an AWS customer in order to carry out security assessments or pen tests against their infrastructure without any prior approval for a maximum of 8 services, listed in the section ‘permitted services’ (See Appendix C).

If there is any security issue found, the customers are not allowed to conduct any security assessments of AWS infrastructure and there is a security issue found during the penetration testing process it needs to be reported to AWS security team immediately. Another important factor is that AWS will inform you if the security testing goes beyond their policy. So, there is no need to take in consideration any issues as performing a penetration test on your own cloud account is allowed free of charge.

**Project Plan**

The project plan is one of the most important parts of the project because all the tasks and steps needs to be known in order for the project to be successful and also to be completed in the time to meet the deadlines. After conducting the research part of the project, I have obtained some important knowledge about the cloud providers and also how cloud pen tests can be achieved. The first thing that will take place after the research will be fully completed will be to decide which services of the AWS are permitted to be tested. The selected cloud provider is one of the easiest to gain permission from because it does not actually require any kind of permission to perform a penetration testing on its cloud platform, but it has a policy that needs to be followed which shows what services can be used when executing a pen test. The next step will be to have a play with the cloud environment and services and to also do some more research around the cloud penetration testing area. The practical work will start as soon as the policy will be conducted and all the permissions needed will be obtained and the cloud environment will be established. The literature review will take place at the same time as the test because the information needed to complete this chapter will be gained from the test execution process, such as the AWS services and the penetration tools used in the project.

A cloud penetration test plan will also be established as it is needed for such a test to be successful. After the plan will be sorted, the pen-test will be carried step by step following the test plan. After the penetration testing will be fully executed and the results will be obtained, the discussions and analysing will take place in order to see what the test outcome was and how can the research question can be answered based on the work done. For the project to be successful, a set of official and non-official deadlines have been established, see Appendix A.

**Appendix A**

Graphical user interface, application, Word

Description automatically generated

**Appendix B**

A picture containing diagram

Description automatically generated

**Amazon Web Services (source: ThinKwik)**

**Appendix C**

Graphical user interface, application

Description automatically generated

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Project Meeting** | **Date** | **Description** |
| **1.** | **Introduction** | **03/03/2022** | **The project proposal discussed and the next project steps** |
| **2.** | **Second Meeting** | **07/03/2022** |  |
| **3.** |  |  |  |
| **4.** |  |  |  |
| **5.** |  |  |  |
| **6.** |  |  |  |
| **7.** |  |  |  |
| **8.** |  |  |  |
| **9.** |  |  |  |
| **10.** |  |  |  |

**Appendix D**

**References**

**Amazon (2022) *Penetration Testing,* AWS Customer Support Policy for Penetration Testing.Available at: hhtps://aws.amazon.com/security/penetration-testing. [Accessed: 20 February 2022].**

**NIST. (2021)** *Final Version of NIST Cloud Computing Definition Published*. Available at: <https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published>. [Accessed: 27 February 2022].

Jain, A. & Mahajan, N. (2017) ‘Introduction to Cloud Computing’. *The Cloud DBA-Oracle.* pp. 3-10.

Singh, S.H., Jeong, Y.S.H. & Park, J.H. (2016). ‘A survey on cloud computing security: Issues threats and solutions’. Journal of Network and Computer Applications. vol.75, pp.200-222.

Yurtseven, I. & Bagriyanik, S. (2020). ‘A Review of Penetration Testing and Vulnerability Assessment in Cloud Environment’. *2020 Turkish National Software Engineering Symposium (UYMS).* pp.1-6.