# Exploring Penetration Testing on Different Cloud Based Services

**Student: Abraham Rey**

**Candidate Number: 215717**

**Supervisor: Imran Khan**

## Aims

Cloud computing has become very popular in recent years and enterprises have become reliant on these types of systems. The reason for appeal is that it's a system with access to a shared pool of configurable computing resources and it offers minimal management effort and/or service provider interaction [1]. Many of the cloud service providers have their own policies when it comes to penetration testing their systems, which restricts us from fully utilising the tools that search for vulnerabilities in a system. As we own the cloud as a service but not as an entity, it can be difficult to perform these tests [1].

This project involves using Kali Linux tools to investigate penetration testing on different CSPs against a vulnerable target and the challenges that may arise while doing so. How complexity differs from pen-testing in a local environment will be explored along with limitations that may appear. During the process, comparing the performance and analysis between systems will be reported.

Motivations for this topic is that cloud security has become more and more relevant and is needed to have more of a priority when it comes to building systems like these.

## Objectives

### Primary Objectives

- Develop an understanding of penetration testing within a cloud-based service, research various CSPs and select which ones to use.
- Design a multi-step process which involves selecting the target we want to exploit, gathering information using various tools within Kali Linux, assess the vulnerabilities in a target, then using all the data gathered in the previous steps we apply and exploit the target; if the exploitation is successful then it's needed to disclose it.
- Assess each penetration test on different services and compare based on how difficult and how much time it took to perform and complete these tests.
- Create a report that describes the process and discuss solutions to any problems or limitations that arises.

### Extension Objectives

- None

## Relevance

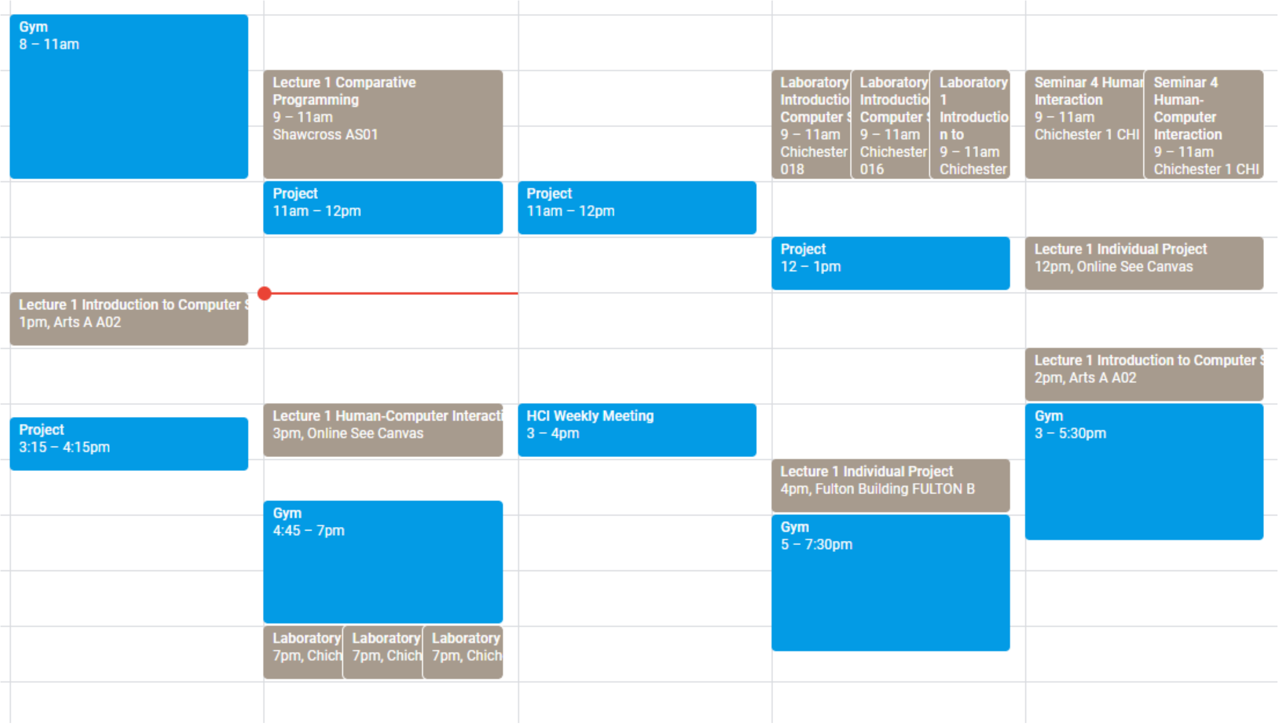
Involving exploiting vulnerabilities in a computer system relates to my Computer Science degree by which one the modules, Introduction to Computer Security, has heavily inspired me to pursue this project. Planning out a well-designed process will test the skills obtained throughout the course, especially in the Software Engineering module; teaching me to take analysis thoroughly and to minimise the risks as much as possible.

Testing also involves scanning a network for information regarding the target, this closely relates to the Computer Networks module. It will give me the ability to evaluate and assess the information gathered from doing so. As someone really interested in security, I want this to be my first security project that shows hard work, dedication as well as a representation of my degree in the past 3 years.

## Resources Required

- VMWare – Virtual Box tool that will help me run the tools needed for testing
    - Need sufficient memory and CPU to run locally
- Cloud based services – web applications needed for the research problem
    - AWS
    - Azure
    - GCP
- Kali Linux tools – contains many tools that helps with penetration testing

## Personal Timetable



Gym
8 – 11am

Lecture 1 Introduction to Computer S
1pm, Arts A A02

Project
3:15 – 4:15pm

Lecture 1 Comparative Programming
9 – 11am
Shawcross AS01

Project
11am – 12pm

Lecture 1 Human-Computer Interacti
3pm, Online See Canvas

Gym
4:45 – 7pm

Laboratory
7pm, Chich

Laboratory
7pm, Chich

Laboratory
7pm, Chich

Project
11am – 12pm

HCI Weekly Meeting
3 – 4pm

Laboratory Introductio Computer S
9 – 11am
Chichester 018

Laboratory Introductio Computer S
9 – 11am
Chichester 016

Laboratory 1 Introductio n to
9 – 11am
Chichester

Project
12 – 1pm

Lecture 1 Individual Project
4pm, Fulton Building FULTON B

Gym
5 – 7:30pm

Seminar 4 Humar Interaction
9 – 11am
Chichester 1 CHI

Seminar 4 Human-Computer Interaction
9 – 11am
Chichester 1 CHI

Lecture 1 Individual Project
12pm, Online See Canvas

Lecture 1 Introduction to Computer S
2pm, Arts A A02

Gym
3 – 5:30pm

## Similar Projects

1. Xu, W., Groves, B. & Kwok, W. (2015). *Penetration testing on cloud---case study with owncloud. Global Journal of Information Technology.* [online] pp. 87-94. Available at: http://dx.doi.org/10.18844/gjit.v5i2.198 [Accessed 19 Oct. 2021]
2. Marabelli, Marco and Newell, Sue (2013). *Managing the outsourcing of information security processes: the 'cloud' solution.* Parallel & Cloud Computing. [online] pp. 24-31. Available at: http://sro.sussex.ac.uk/id/eprint/49696/ [Accessed 19 Oct. 2021]

## Bibliography

1. Stallings, W. and Brown, L., *Computer Security Principles and* Practice (2018), 4th Edition, Pearson, Hudson Street, New York, pp. 446-470 [Accessed 15 Oct. 2021]
2. Khawaja, G. (2018). *Practical Web Penetration Testing*. Packt Publishing. Birmingham. [online] pp. 187-206 [Accessed 16 Oct. 2021]
3. *Intranet* (2021), [Online] Available at: https://en.wikipedia.org/wiki/Intranet [Accessed 16 Oct. 2021]
4. Posey, B., *IoT devices (internet of things devices)* (2021), [Online] Available at: https://internetofthingsagenda.techtarget.com/definition/IoT-device [Accessed 16 Oct. 2021]
5. Gregg. M., *Zone Transfer* (2006), [Online] Available at: https://www.sciencedirect.com/topics/computer-science/zone-transfer#:~:text=Zone%20transfer%20is%20the%20process,in%20a%20secondary%20DNS%20server. [Accessed 16 Oct. 2021]
6. Steve, *DNS Zones and Zone Files Explained* (2020), [Online] Available at: http://www.steves-internet-guide.com/dns-zones-explained/#:~:text=A%20zone%20file%20is%20a,to%20the%20other%20DNS%20servers. [Accessed 16 Oct. 2021]
7. *Listener*, [Online] Available at: https://docs.rapid7.com/metasploit/listeners/ [Accessed 16 Oct. 2021]
8. Varghese, J., *A Complete Guide on Cloud Penetration Testing* (2021), [Online] Available at: https://sussex.primo.exlibrisgroup.com/discovery/fulldisplay?docid=cdi_askewsholts_vlebooks_9781788628723&context=PC&vid=44SUS_INST:44SUS_VU1&lang=en&search_scope=MyInst_and_CI_no_BLDS&adaptor=Primo%20Central&tab=MyInst_and_CI_no_BLDS&query=any,contains,Gus%20Khawaja&offset=0 [Accessed 17 Oct. 2021]
9. *Penetration Testing Methodologies*, [Online] Available at: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies [Accessed 17 Oct. 2021]
10. Caudill, B., *Penetration Testing in the AWS Cloud: What you Need to Know*, [Online] Available at: https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-cloud-need-know/ [Accessed 17 Oct. 2021]
11. *What is PCI?*, [Online] Available at: https://www.pcicomplianceguide.org/faq/#1 [Accessed 17 Oct. 2021]

# Interim Log

## Meeting #1 (29/09/2021) – Initial meeting with supervisor:

- Discussed general project
- Looked at previous Networks coursework
- Decided to use Kali Linux
- Use tutorials and videos to get a basic understanding

## Meeting #2 (08/10/2021) – Group meeting with supervisor:

- Looking at examples of previous projects
- Discussing project proposition
    - Aims and Objectives
- Complexity is important
- Similarities with other projects
- Limitations of pen testing tools against a target in AWS (cloud-based environment)
    - Pen testing tools
    - Frameworks/pen testing methodologies
    - Do they work as effectively in a cloud environment rather than a local one?
    - Comparisons between the frameworks, create a new framework

## Meeting #3 (14/10/2021) – Discussion on project proposal:

- Research about cloud-based security and penetration testing
- Formulate a project proposal by the end of the week