Penetration Testing on Different Cloud Based Services

Candidate Number: 215717

October 30, 2021

Contents

1 Introduction

Cloud computing has become increasingly popular over several years and enterprises have become more reliant on these types of systems. These types of services provide you access to a shared pool of configurable computing resources over a network. What makes it so attractive is that it offers minimal management effort and/or service provider interaction [30].

Vulnerabilities in clouds are present due to many reasons. APIs, which are insecure, may have lack of input sanitisation and improper access control; servers are misconfigured, weak credentials, outdated software and even coding practices that are insecure [33]. All these may be exploited and potentially lead to integrity and confidentiality breaches on sensitive data.

In penetration testing, information is gathered about a target and uses this data to search for vulnerabilities. These are exploited and ultimately achieve remote access and root (administrator) privileges in the target's system [20].

In this project we are exploring penetration testing on popular Cloud Service Providers (CSPs) such as AWS, Azure, and GCP. We will be using an open-source security package named Kali Linux containing tools divided by a number of categories [32]. Our problem area is discussing whether different CSPs affect the capacity and difficulty to conduct penetration tests against a vulnerable target. We will be setting up virtual machines within each CSP and use them as targets for our penetration testing. In carrying out this investigation we will face some challenges, most dominantly are the policy restrictions specified by each CSP. They define the endpoints and types of tests that may and may not be performed [33].

1.1 Aims and Objectives

Reading Literature I will gain knowledge on cloud computing, in order to attain a thorough and well-put report of my results. Learning how to use Kali Linux and its various tools will be required, in order to be able to gain a familiarity with penetration testing.

Design A Multi-Step Process This aims to create a thorough plan that involves selecting the target we want to exploit, gather information using Kali Linux and assess the vulnerabilities. Using all the data gathered, we exploit the said target and if successful then it is needed to be disclosed/reported. I will also plan around the restrictions each cloud service may have (e.g. which endpoints to exclude based on policy, user permissions etc.) [33].

Assess Each Penetration Test On Different CSPs The main aim of this project is to compare multiple factors such as difficulty, complexity etc. with regard to penetration testing on different cloud service providers.

Report Exploited Vulnerabilities This is simply to gather the data that we have accumulated and display the vulnerabilities in an understandable way that is readable to a user. It is needed to be 'well-organized and categorized' based on 'type' and 'level of threat' [33]. Getting in touch with the developers if any new vulnerabilities are discovered will be important depending on the level of threat it has when exploited.

Analyse Effectiveness Of The Process This focuses on the results produced, discussing how effective it was to carry out the investigation. We will also consider any improvements on our methods so that penetration tests would potentially be more thorough and faster.

1.2 Motivations

Security in cloud services is a problem that needs to be addressed and prioritised more due popularity of these systems. My motivation in this topic stems from this.

Researching into this topic will allow me to gain experience and knowledge in security as well as develop my networking skills. Pen-testing involves scanning a network in order to gather information about a target; this closely relates to the Computer Networks module. Applying the knowledge I had from that course will assist me when evaluating and assessing the data.

As someone interested in security, I want this to be my first project relevant to the subject, that shows hard work, dedication as well as a representation of my degree in the past 3 years. This will be significant to have in my portfolio as it will exhibit what I have learnt to my future employers.

2 Professional Considerations

2.1 BCS Code of Conduct

This project will be closely guided by the BCS Code of Conduct with the relevant sections [12]:

“1(a) Have due regard for public health, privacy, security and well being of others and the environment. ”

No human participants shall be involved as the policies of the cloud services restrict us from performing tests that involve others [33].

“1(b) Have due regard for the legitimate rights of Third Parties* . ”

We will be using several third party tools, most importantly cloud services which have several policies that shall be taken in to consideration and to be followed.

“1(c) Conduct your professional activities without discrimination on the grounds of sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or disability, or of any other condition or requirement. ”

During our investigation, the project shall not discriminate on any account.

“1(d) promote equal access to the benefits of IT and seek to promote the inclusion of all sectors in society wherever opportunities arise. ”

In terms of promoting the benefits of IT, the project will showcase cloud-security in a sense that may possibly further improve if any flaws are discovered.

“2(a) Only undertake to do work or provide a service that is within your professional competence. ”

“2(b) NOT claim any level of competence that you do not possess. ”

As discussed with my technical supervisor, I possess the ability to undertake this project in accordance to 2(a) and 2(b). In order to do so I must actively learn about the subject as well as use previous knowledge from my previous modules such as the Computer Networks and Software Engineering.

“2(c) Develop your professional knowledge, skills and competence on a continuing basis, maintaining awareness of technological developments, procedures, and standards that are relevant to your field. ”

Researching and learning about the topic while carrying out the task will help develop my skills. As well as being aware of other similar projects that involve cloud-computing and penetration testing.

“2(d) Ensure that you have the knowledge and understanding of Legislation* and that you comply with such Legislation, in carrying out your professional responsibilities. ”

Again, the policies of the cloud-services shall be complied and followed during the project’s process.

“2(e) Respect and value alternative viewpoints and, seek, accept and offer honest criticisms of work. ”

Seeking constant and consistent feedback from my technical supervisor as well as others interested in the subject at significant points in the project will be necessary. Taking criticism from others is important because it will help me build on what I have already learned and develop my relevant skills.

“2(g) Reject and will not make any offer of bribery or unethical inducement. ”

I shall not undertake any offer of bribery or unethical inducement as well as entice it.

2.2 Ethical Review

This investigation does not involve any human participants and therefore does not need an ethical review at this time of writing; as discussed with my technical supervisor.

3 Research

3.1 Background Reading

3.1.1 Properties of Cloud Computing [30]

Cloud computing provides broad network access through the use of multiple platforms such as phones and laptops;

It also allows for rapid elasticity which means to expand or reduce the resources according to the service requirement. For example, a large number of resources are used for a duration of a complex task and are released after completion.

Transparency is assured for both the provider and consumer as control and the optimisation of resources are automated. The storage, processing, bandwidth and active user accounts etc. are all monitored, controlled and reported. This would add a level of security to the services used.

A Cloud Service Consumer (CSC) involves the provision of computing capabilities (e.g. server time and network storage). This process is automatic which means no human interaction is needed with each service provider. It is also on-demand so that resources are not permanent to the CSC. We will be efficient as possible when using the cloud service resources because most (if not all) require a payment or subscription of some type.

Multiple CSCs are served by a multi-tenant model, which is a "single instance of the software and its supporting infrastructure" or cloud, "that serves multiple customers " [18]. Different physical and virtual resources are assigned to each user according to their demands. At the security level, the CSC has no awareness of the exact location of the provided resources, but they may be able to find country, state, or data centre etc. Depending on our complexity of pen testing vulnerabilities we may need more or less cloud resources which can affect the time and cost of the project.

3.1.2 Network Penetration Testing [20]

Penetration testing has many phases, starting with information gathering;

There are two types: passive and active. Passive involves no direct contact with the chosen target whereas active otherwise does [14].

Passive Information Gathering To start the process we passively gather; or research about the target's online presence. This is also called the 'Open-Source Intelligence (OSINT)', referring to the data collected from the internet. We first find details about the company, employee, and the web application being used without direct contact with the target. Examples such as location, DNS, names, email addresses, programming languages used etc. are all useful data. Most of the information is found on the target's website.

When researching online with search engines, Google isn't the only option. We may also use ones from other regions such as China [1] or Russia [8]. The TOR network (dark web) can be used to search but we will not consider this as we will be carrying out basic penetration tests.

Within this project, we will be using most of the tools from Kali Linux that are used for information gathering. As stated, some tools may not be available so we may need to access the resources and download them from GitHub [3].

Another tool that may be useful is called Google Dorks [4]. This is a query search engine that is used to reveal sensitive information about a target where various goals are achieved. These include revealing sensitive directories, target network's vulnerabilities data, web server information, credentials and confidential data, etc.

Using a WHOIS lookup (a database where every domain name is registered to), can be proved useful. We can reveal a considerable amount of information such as names, phone numbers, emails etc.

Domain Name System (DNS) is used to determine its corresponding IP address. Information can also be retrieved from it, an example would be to "identify if whether the DNS server allows a zone transfer". A zone transfer is the process of copying contents of a zone file from a primary to a secondary DNS server [28] (a zone file is a "text based file with a format defined in RFC 1035 and 1034, stored on a DNS server" [31]).This zone file contains the IP addresses and host name data of the internet-accessible systems which are revealed if zone transfers are permitted. There are also various other data we can gather from using DNS.

Active Information Gathering In this phase we gather data about live hosts and all the services running on those hosts. A four-step process is involved: first we get the IPs/ranges from the client or employer, identify the live hosts, list the open ports/services on each host and then monitor each service for more information. All these can be completed using the Nmap tool made available on Kali Linux.

Vulnerability Assessment Some Nmap scripts checks for vulnerabilities however as stated by in an 'enterprise environment', automatic scanners would instead be used (Nessus or Nexpose). Within the cloud, there are scanners also available from these companies such as InsightVM. Our goal here is to identify the vulnerabilities and check if they're not false positives; that they exist.

Exploitation In this phase we take the vulnerability and exploit it; in turn we get a remote shell up and running on the target machine.

There are many options to find most exploits, however Metasploit will be the main database that I will be using as the framework is both free and comes pre-installed in Kali Linux.

Before uploading and executing the payload we will set up a listener (this waits for an incoming connection from an exploited system [26]). This is needed so that we can create a connection between our server and the target machine.

Next, a script will generate a shell payload based on what operating system is being used such as Linux or Windows; custom shells are also available (Bash etc). We may need to also elevate our privileges on to the exploited machine, as we may get a limited shell. Achieving administrator rights, we transfer a script on to the user's machine using the limited shell, this will be described in detail in the implementation.

3.1.3 Penetration Testing in Cloud-based Services [33]

Carrying out penetration testing through a cloud would require a few more steps described previously. Before we carry out any task that involves planning, we would need to be aware of the policies of the cloud service provider that we will be using and understand them.

Planning After this, we create a testing plan that maps out the endpoints such as user interface, APIs, subnetworks etc; excluding those based on policy, user permissions and such. We then decide to perform the penetration test from either the application or database. How well the application server and VMs can take the load of our tests will also be a factor on what kind of test we'd like to perform; as well as laws that needed to be acted in accordance with. Tools are then chosen and whether they are automated or manual, on different endpoints. It is recommended to "get approval for your plan from the client and inform them when you wish to begin" but we will not need to as our penetration tests will not involve any human participants. We will be using a tool called Mutillidae from OWASP which is a web application that is deliberately vulnerable [15].

Executing the plan will allow us to "observe the responses for vulnerability", and there are multiple CSP-specific tools that we may use such as AWS Inspector.

Verifying False Positives It is important to verify the false positives in the cloud because we don't want to generate incorrect information in the final report. We then repeat this for each network layer that we are testing ("seven layers that computer systems use to communicate over a network" [7]).

Report Generation The next stage is report generation, and it is needed for the vulnerabilities to be presented in an "understandable matter" so that the 'client' viewing the information will take it seriously or not. We categorize it based on the "type and level of threat", leading to a well organized document. We may contact the developers to patch the vulnerabilities but we will be already pen testing using a practice tool already mentioned previously; so this step is not needed. However, this can be made into a desirable requirement if we were to improve our investigation.

3.1.4 Penetration Testing in the AWS Cloud [22]

In this section we will be describing the steps taken to specifically penetration test using the AWS cloud service provider.

About AWS The cloud platform has "90 different cloud hosting services", including network infrastructure. The platform in which we build our environment cannot be penetration tested; this suggests that we need to use external third-party code or assets in our environment.

Policies There are several testing functions that are not/permitted described;

Described as 'User-Operated Services', it is permitted to create cloud offerings that are managed by the user; however this excludes disrupting network traffic via DOS/DDOS attacks.

'Vendor Operated Services' are third-party services that are not part of the "underlying infrastructure" of the cloud such as Cloudfront where the hosting infrastructure is not allowed to be pen tested. They are limited by the “implementation and configuration of the cloud environment”; this is a challenge that we may face during our testing when carefully choosing what services we need. In our project we will be using the Elastic Cloud Computing (EC2) instance in AWS. A list of what can be tested is shown: APIs (HTTP/HTTPs for example), web and mobile applications hosted by our organization (not applicable to this project), application server and associated stack such as Python, and VMs & operating systems. What can’t be tested also appears, referring to the “legal and technological constraints”: services, applications, physical hardware, underlying infrastructure, or facility that belongs to AWS, EC2 environments owned by other organizations, appliances that are managed by other vendors without permission. The policies that restrict us involve the surrounding business of AWS and as long as we do not disturb this, following the policies then we can carry out our penetration tests safely.

Differences From Traditional Penetration Testing We shall be aware of the differences from traditionally penetration testing outside of clouds. As what is normal to do in ’ethical hacking’, may not align with the policies within AWS and may violate them. It must all be focused on the user’s assets they have ownership with, as well as many others.

3.1.5 Web Application Vulnerabilities [20]

Several different attacks are carried out in web applications, here are a few that are described;

File Inclusion This is a type of attack that involves a file in the URL. There are two types: local file inclusion or remote file inclusion. As the name suggests, local file inclusion uses the file that is local to the application’s server. On the other hand, remote file inclusion uses a path to point to a remote file that is outside the boundaries of the web server (e.g. attacker’s own malicious file).

It is noted that local file inclusion allows for “directory traversal” character to be injected into the URL (e.g. ../), which can be used to access certain files such as stored passwords.

Cross-Site Scripting Also named XSS, this vulnerability is exploited when the attacker can “successfully execute any type of script on the victim’s browser”; JavaScript is most common. They are able to perform this as requests weren’t properly validated or the encoded response of the application was incorrect. Three types are used: stored, reflected and DOM XSS. Mutillidae [15] can be used to practice revealing these types vulnerabilities.

Stored XSS A script is saved into a stored location/file (e.g. database) through a web page and is executed when someone visits the infected page. An interesting aspect to this type is that you can exploit it using the network packet headers.

Reflected XSS The URL of a page or some body inside such as a search bar, can be used to change what the user sees on their display where it can be “manipulated dynamically”. The script is then executed when the user confirms an input such as a button.

DOM XSS In this type we use JavaScript instead of HTML (as used in the previous two types) to inject our script. By inspecting the code in the page we change and inject the script to perform our malicious action. This results in the script executing as soon as the user loads the web page.

3.2 Related Work

In this section we will be discussing example projects/papers that are similar to ours, so that we can get a better understanding of cloud penetration testing.

3.2.1 Penetration Testing on Cloud - Case Study with ownCloud [35]

In this paper, it emphasises the importance to test the "security threats and check what the possible risks that these threats may bring" in a cloud computing infrastructure. The problem area they discuss is finding whether "it is the problem of cloud computing server or the problem of cloud itself" when hacking is involved.

They perform three different main attacks where some were successful and some were not;

Man-in-the-middle The first is a man-in-the-middle attack by which they get the contents of an image file sent from their Windows 7 VM their ownCloud server machine by intercepting it. This resulted it into success and captured the image as it was being uploaded. In our project, we may consider using this specific type of vulnerability.

SQL Injection Secondly, an SQL injection attack is performed (taking advantage of SQL code used for queries we can maliciously access the database and manipulate it to access potentially confidential information or to destroy sensitive data [19]). In their methods, they were unsuccessful in performing the attack; this can be due to many reasons which will be discussed in our own tests.

Administrator Account In their last series of attacks, they try to gain access to computer resources in order to gain access to their ownCloud administrator account. This was also successful as they were able to use a key logger that was able to record the keystrokes of the user as they were typing in their credentials. This type of tool may be proven useful to us as well.

Conclusion We will be similarly performing these types of tests on each cloud service. It is important that we keep parameters used in the tests the same or very close to each other (e.g. tools, targets etc), in order to maintain fair and unbiased results during comparison.

3.2.2 Cloud Penetration Testing [21]

Here is another project that attempts to perform several penetration tests within the OpenStack Essex Cloud Management Software.

They mention that OpenStack includes CSPs offering Infrastructure as a Service (IaaS). Organisations use this type of service to rent servers for resources and storage within the cloud [24]. Instead for our project we will be using the Platform as a Service (PaaS), describing hardware and software tools that are provided for us. This is appropriate for information security as we don't need to install local software to run our tests [34].

The paper analyses the software thoroughly, discussing its various tools such as networking, storage and image management. We will be performing similar tasks in order to achieve a better understanding of the software that we will be using.

Session Hijacking Describing the first attack, called session hijacking said to involve "the exploitation of a valid session key to gain unauthorized access to a computer system or a computer network. " A HTTP session is started with a server over a network connection. When a request is sent, a session key is returned back to the user from the server. This is used so that the user doesn't need to login with their details but instead use their private key. With packet sniffing (reads the packet in between IP destinations), the attacker can access the session key. Unrestricted access to the user's web page is granted for the attacker. We will use this technique in our project through Metasploit [5].

Credential Theft The next attack describes user credentials that are stored in an non-secure way (unencrypted files or plaintext). These files can be transmitted over a network, allowing the attacker to gain access to the user's account. Use of a key logger as previously described in the first paper [35], is also used to record the keystrokes of the user to reveal their details.

Implementation They first start by implementing two machines within a cloud using one network interface to connect the OpenStack server to an Internet Gateway (allowing communication between the cloud and the internet [29]), and the second to connect the server to the other computers.

The system Backtrack 5 (R3) was used as it has multiple penetration tools similar to Kali Linux, they use a network scanner (Zenmap) to reveal all the network ports available to attack. This was then used to organise the network packet structures for each port; to perform the appropriate penetration tests.

Using session hijacking they steal the user's session cookie from their HTTP session. Cookies are a form of data that are stored onto the user's local computer from a website that they visit such as name, home address, email etc [2]. Using a program called Ferret, it monitors the connection between the user and server; capturing the session cookie. It is stored in a text file and URL information (web pages visited). Regarding their penetration test, they test the vulnerability patch by OpenStack where they reset the session cookies after a user logs out, and removes them.

They found that the patch didn't prevent this while the user was logged in; session hijacking was still executed and the session cookie was stolen. Unauthorized access was granted to the attacker and was able to use web pages within the user's account. This issue was reported to the OpenStack developers and suggested that a secure network protocol like HTTPS is used.

Conclusion Through this paper we have learnt how penetration planning and implementation is carried out within a cloud environment, in a real scenario. We will apply some of these techniques such as packet sniffing in our investigation.

3.3 Tools and Resources

3.3.1 Cloud Service Providers

All three providers provide free tiers which allow us to use certain services for an amount of time or specified monthly usage limits.

AWS gives us free 750 hours of the EC2 instance (compute power). Azure provides 12 months of free usage for a variety of services including Linux-based VMs. GCP also offers a free tier where you can use an e2-micro instance until a number of hours has been used in the current month. It also alternatively offers credit for 90 days for their free trial [11, 23, 16].

Amazon Web Services (AWS) Amazon gives us Elastic Compute Cloud (EC2) instances which are virtual servers used to run applications within AWS. We will use this to set up a virtual machine based in Linux. A particular feature called elastic IP addresses allows us to associate an IP addresses with a single instance and can be moved in between instances; this will be useful for us if we want to gather information between two hosts [13].

Multiple types are given in an EC2 instance and we will be using a type T2 instance providing a "baseline level of CPU performance with ability to burst above the baseline ". They suggest it is a good choice for general-purpose workloads which includes virtual desktops [10].

Azure Azure also has a similar VM within the B-series, specifically the B1s size offering similar features to T2.micro EC2 instance in AWS. Ideal workloads which don't continuously need the full performance of the CPU and allows us to burst above the baseline [27].

Google Cloud Platform (GCP) In Google's cloud free program they offer an e2-micro instance and as previously described, allow us to use it until a certain max time in the current month has been used. This means we have to be efficient in our planning as possible so that we get the most out of it. We are also given $300 in free credits used to run our workloads [17].

3.3.2 Environment - Kali Linux

We will set up Kali Linux on a local machine, via VirtualBox [6] and penetration test against each target relative to their CSP. There are various tools in which we will use for learning about and carrying out our tests.

Metasploit [25] Metasploit is an open-source penetration testing framework that contains various tools. Pre-installed with Kali Linux, it provides scanning and exploiting tools. Scanners such as Nmap and SNMP scanning are included (used for the information gathering phase).

Its large database contains information used to exploit the potential vulnerabilities found. A payload is then sent (such as a shell), to the target machine. As mentioned before in our background reading, it also provides us with packet sniffing and keyloggers.

We will use this as it is all contained in one package and gives us enough tools to execute thorough penetration tests.

OWASP Mutillidae II [15] Mutillidae II is a free open-source, deliberately vulnerable web application. It can be used for learning penetration testing and can act as a target for our investigation.

It contains over 40 vulnerabilities, at least one for each of the OWASP Top Ten 2007, 2010, 2013, and 2017 (a document containing the top security risks in the current year [9]). It is also a training application that provides tutorials and hints that help us exploit the dummy vulnerabilities.

I will install this on a Linux virtual machine for each cloud service provider.

4 Requirements

As already stated in our aims and objectives our project will be set to carry out penetration tests against a specific vulnerable target (i.e. Mutillidae II). We will use Kali Linux against Linux-based virtual machines created within each CSP: AWS, Azure and GCP.

I have organised our requirements into two sections, mandatory which must be completed and desirable which aren't expected to be completed.

4.1 Mandatory

1. We shall research and practice penetration testing and vulnerabilities in order to gain a better understanding around the area, through the use of Mutillidae II.
2. We shall set up Kali Linux on a local desktop/machine.
3. We shall set up Linux-based machines for each CSP (AWS, Azure and GCP).
4. We shall install Mutillidae II on to each VM.
5. We shall learn how to use Metasploit on Kali Linux and its various tools.
6. We shall write a test plan that will carry out our penetration tests for each system, with consideration of the policies from each CSP.
7. There shall be 3 different vulnerabilities that will be tested.
8. We shall attempt to get a Linux shell payload onto each system and achieve administrator access.
9. We shall write exploited vulnerability reports for each test.
10. We shall assess the success and compare the results for each CSP based on factors: difficulty, complexity, time and efficiency.

4.2 Desirable

11. We should compare how effective penetration testing is in a local environment compared to a cloud environment.
12. We should carry out a real penetration test in an attempt to find vulnerabilities.
13. We should report to the developers if such vulnerabilities are found.

5 Project Plan

5.1 Tasks and Gantt Chart

Referring to Figure 1, a gantt chart is created to show the outline of our project plan; presenting a parallel approach to our problem area.

1. Project Selection Process of selecting our project and our techincal supervisor.

2. Research Learning about penetration testing and cloud computing. More will need to be carried out in order to execute the subsequent tasks.

3. Project Proposal A document that proposes our project describing our objectives and how we plan to meet them.

4. Interim Report A document that formally outlines the project with research, requirements and planning; formed as an extension of the project proposal.

5. Setup Environments Set up the various environments as described in our mandatory requirements (Kali Linux, Metasploit, CSPs etc).

6. Test Plan Writing a formal plan describing how we will be carrying out our penetration tests.

7. Implementation Execution of our test plan.

8. Vulnerability Reports Assessing the exploited vulnerabilities on their success.

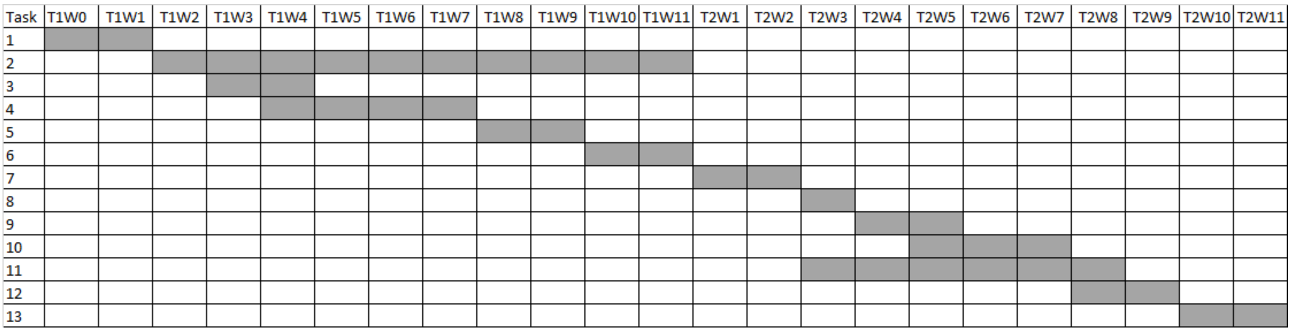
9. Results Analysis Conclusion of our results in comparing with each CSP.

10. Expert Feedback As a result we will contact one or two experts to evaluate our findings.

11. Draft Report Working version of our final report, submitted 3 weeks before the final deadline to our supervisor.

12. Poster Creation Used to present our final project in the poster event.

13. Final Report We will finish our final report in the final weeks, looking at the feedback from our technical supervisor and implementing changes.



Task	T1W0	T1W1	T1W2	T1W3	T1W4	T1W5	T1W6	T1W7	T1W8	T1W9	T1W10	T1W11	T2W1	T2W2	T2W3	T2W4	T2W5	T2W6	T2W7	T2W8	T2W9	T2W10	T2W11
1	▨	▨																					
2			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨											
3				▨	▨																		
4					▨	▨	▨	▨															
5									▨	▨													
6											▨	▨											
7													▨	▨									
8															▨								
9																▨	▨						
10																	▨	▨	▨				
11															▨	▨	▨	▨	▨	▨			
12																				▨	▨		
13																						▨	▨

Figure 1: Gantt Chart of the Project Plan

I have designed our Gantt chart while keeping in mind our time constraints make sure we are organised and is well set for our project implementation.

At the time of writing this report, we have researched about the basics of network penetration testing, penetration testing on cloud-based services, penetration testing within the AWS cloud, and example web application vulnerabilities. We have also looked at related works that have been carried out with regards to penetration testing on cloud platforms. We will carry out further research as stated in our requirements and in our project plan. This will mostly cover penetration testing practice.

6 References

[1] Baidu Search Engine. https://www.baidu.com/.

[2] Cookies. https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer.

[3] GitHub. https://github.com.

[4] Google Dorks. https://www.exploit-db.com/.

[5] Metasploit | penetration testing software, pen testing security. https://www.metasploit.com/.

[6] Oracle VM VirtualBox. https://www.virtualbox.org/.

[7] What is OSI model | 7 layers explained. https://www.imperva.com/learn/application-security/osi-model/.

[8] Yandex Search Engine. https://yandex.com.

[9] OWASP top ten web application security risks. https://owasp.org/www-project-top-ten/, 2021.

[10] Amazon. Amazon EC2 instance types. https://aws.amazon.com/ec2/instance-types/.

[11] Amazon. Free cloud computing services - AWS free tier. https://aws.amazon.com/free/.

[12] British Computing Society. BCS Code of Conduct. https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/, 2021.

[13] TechTarget Contributor. What is an amazon EC2 instance? https://searchaws.techtarget.com/definition/Amazon-EC2-instances, 2021.

[14] Ivan Dimov. Information Gathering. https://resources.infosecinstitute.com/topic/information-gathering/, 2019.

[15] Jeremy Druin. OWASP mutillidae II. https://github.com/webpwnized/mutillidae. original-date: 2018-09-28T02:41:14Z.

[16] Google. Google cloud free program. https://cloud.google.com/free/docs/gcp-free-tier.

[17] Google. Machine families | compute engine documentation. https://cloud.google.com/compute/docs/machine-types.

[18] Digital Guardian. SaaS: Single tenant vs multi-tenant - what's the difference? https://digitalguardian.com/blog/saas-single-tenant-vs-multi-tenant-whats-difference, 2020.

[19] Imperva. What is SQL injection. https://www.imperva.com/learn/application-security/sql-injection-sqli/.

[20] Gus Khawaja. *Practical Web Penetration Testing: Secure Web Applications Using Burp Suite, Nmap, Metasploit, and More.* Packt Publishing, Limited, 2018.

[21] Ralph LaBarge and Thomas McGuire. Cloud penetration testing. 2013.

[22] Rhino Security Labs. Penetration testing in the AWS cloud: What you need to know. https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-cloud-need-know/, 2017.

[23] Microsoft. Create your azure free account today. https://azure.microsoft.com/en-gb/free/.

[24] Avi Networks. What is infrastructure as a service (IaaS)? https://www-stage.avinetworks.com/glossary/infrastructure-as-a-service-iaas/.

[25] J. M. Porup. What is metasploit? and how to use this popular hacking tool. https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html, 2019.

[26] Rapid7. Listener | metasploit documentation. https://docs.rapid7.com/metasploit/listeners/.

[27] rishabv90. B-series burstable - azure virtual machines. https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-b-series-burstable, 2021.

[28] ScienceDirect. Zone transfer - an overview. `https://www.sciencedirect.com/topics/computer-science/zone-transfer`, 2008.

[29] Amazon Web Services. Internet gateways. `https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html`, 2021.

[30] William Stallings and Lawrie Brown. *Computer Security: Principles and Practice, EBook, Global Edition*. Pearson Education, Limited, 2017.

[31] Steve. DNS zones and zone files explained. `http://www.steves-internet-guide.com/dns-zones-explained/`, 2017.

[32] Tutorialspoint. Kali linux tutorial. `https://www.tutorialspoint.com/kali_linux/index.htm`.

[33] Jinson Varghese. A complete guide on cloud penetration testing. `https://www.getastra.com/blog/security-audit/cloud-penetration-testing/`, 2021.

[34] Chai Wesley, Kate Brush, and Bigelow Stephen J. What is PaaS? `https://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS`, 2021.

[35] Wenjuan Xu, Brian Groves, and Willson Kwok. Penetration Testing On Cloud - Case Study With owncloud. *Global Journal of Information Technology: Emerging Technologies*, 5(2):87–94, 2015. Number: 2.

7 Appendices

7.1 Appendix 1: Interim Log

7.1.1 Meeting #1 (29/09/2021) - Initial meeting with supervisor

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

7.1.2 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

7.1.3 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

7.2 Appendix 2: Proposal Document

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

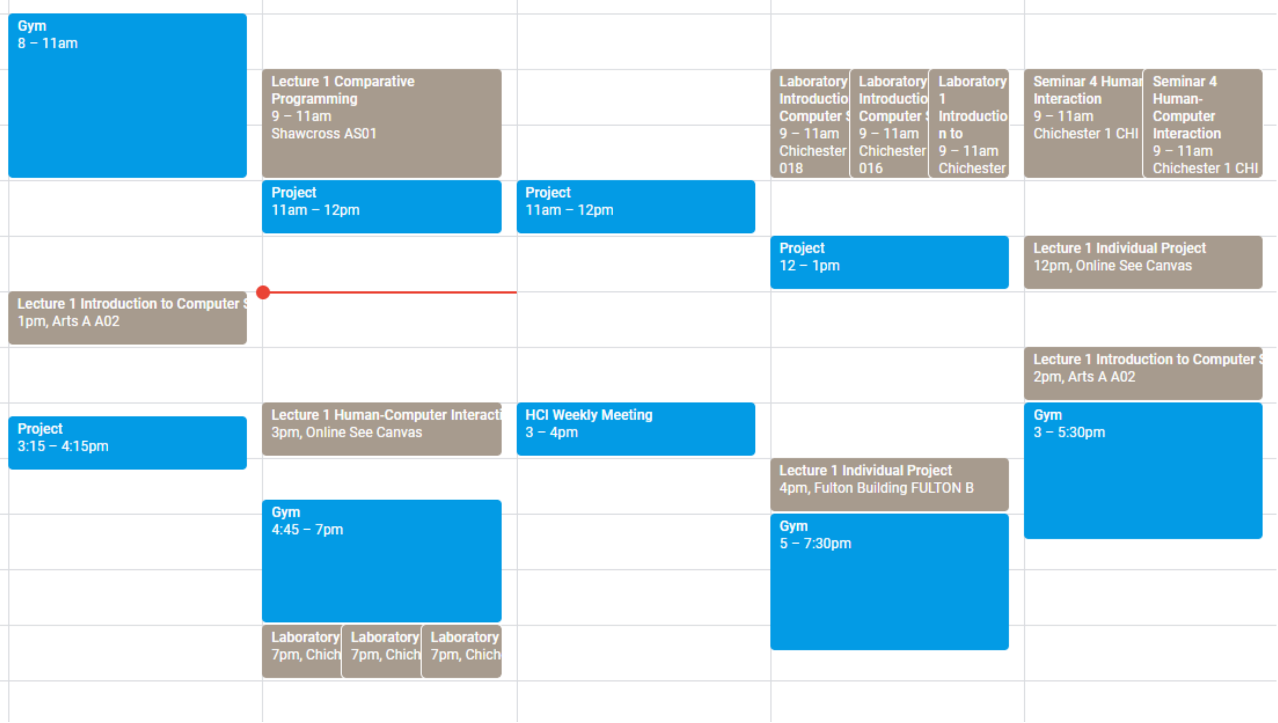
Involving exploiting vulnerabilities in a computer system relates to my Computer Science degree by which one the modules, Introduction to Computer Security, has heavily inspired me to pursue this project. Planning out a well-designed process will test the skills obtained throughout the course, especially 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 Human
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