Partners Universal International Research Journal (PUIRJ)
Volume: 02 Issue: 01 | January-March 2023 | ISSN: 2583-5602 | www.puirj.com

Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments

A.Shaji George[1], S.Sagayarajan[2]

[1,2]*Independent Researcher, Chennai, Tamil Nadu, India.*

Abstract – Cloud computing is rapidly becoming the go-to platform for businesses of all sizes, from start-ups to large enterprises. With this shift comes a responsibility to ensure that cloud applications are secure and can protect data from malicious actors. Joint responsibility model of cloud security says that while service providers have to make sure their services are secure, businesses that use those services must also take steps to maintain their own level of security. Identity as well as access management is a shared responsibility model that offloads some of the application security responsibilities to the client. It is important to understand the impact of such a system when it comes to protecting confidential data from malicious attacks. This includes putting in place protocols for identity as well as access management and doing ethical hacking and penetration testing to make sure that the most data protection is possible. Cloud security has become a joint responsibility between the user and the provider, so it is essential for clients to take responsibility for the security of their cloud applications. This mainly applies to IaaS and PaaS services. In order to ensure a secure virtual environment, advanced security measures such as ethical hacking and penetration testing are a must. These efforts will enable organizations to stay safe from malicious attacks and data leakage. Penetration testing for cloud-based assets is an effective way to increase risk visibility, discover vulnerabilities, control risks, and gain valuable telemetry data to ensure better security. The main objective of this research paper is to evaluate the methods used in hacking cloud applications while also developing a framework or checklist to identify associated risks and vulnerabilities. This will help keep cloud-based apps secure from malicious actors.

Keywords: cloud penetration testing, cloud security challenges, secure cloud services, secure cloud infrastructure, securing virtual machines and containers on public clouds, identifying vulnerabilities in AI-enabled applications on clouds, a zero-trust model to protect data stored in clouds, cloud-based application testing challenges, and penetration testing challenges in IaaS/PaaS/SaaS environments.

1. INTRODUCTION TO CLOUD COMPUTING AND ITS USAGE IN BUSINESS

Cloud computing has completely transformed the way companies function, enabling them to make the most of resources, maximize efficiency, and develop innovative solutions. Cloud computing is a technology that enables companies to store and access data, applications, and other resources on the internet rather than having to use their own physical servers. In order to ensure data safety and reliability, businesses are increasingly turning towards cloud computing systems. This also places a weight of responsibility on the organization to adopt robust measures for securing their cloud infrastructure from cyber threats. This allows companies to save money by avoiding costly investments in hardware infrastructure while still being able to use powerful services such as software-as-a-service (SaaS), platform-as-a-service (PaaS), or infrastructure-as-a-service (IaaS). Cloud computing provides businesses with an array of benefits, not the least of which is

 |DOI:10.5281/zenodo.7723187

scalability. Companies can scale up or down as and when required without purchasing additional hardware and equipment. This saves time, effort, and more importantly, money.

Cloud computing is a valuable asset for many businesses. It has various uses, such as saving and backing up data, hosting websites and web applications, running analytics programs, and granting employees access to virtual desktops so they can work remotely. Cloud storage is a cost-effective alternative to buying hard drives for each user, as files are stored remotely instead. Additionally, cloud platforms take care of software updates automatically without any manual intervention. Utilizing modern IT systems can save businesses time and money when it comes to maintenance. As updates are automated, there's no need for manual intervention compared to traditional systems.

It's essential to be aware of the security that cloud providers provide. Their services come with strong encryption to protect your data and ensure its privacy and safety. Companies use multiple levels of authentication protocols and encrypted connections to protect sensitive data on their networks from potential cyberattacks. These techniques help keep the information safe from unauthorized access by adding another layer of security. In general, these areas tend to be very secure and provide a safe working environment. Due to the evident benefits, many companies have been turning towards utilizing AI writing assistants rather than traditional methods. This allows them to become much more efficient financially and operationally as they are provided with a higher degree of protection. Security is a key consideration in cloud computing, and while cloud providers can offer more comprehensive security features, it is ultimately the responsibility of organizations to ensure the safety and security of their data stored in the cloud.

2. OBJECTIVE

The goal of cloud application infrastructure security is to protect data and resources from security risks and threats. Penetration testing is a key part of cloud security because it helps find weaknesses and holes in the system. But doing penetration testing in an IaaS, PaaS, or SaaS environment comes with its own set of challenges.

- In an IaaS environment,[24] the customer is responsible for keeping the data, operating systems, and applications running on the cloud infrastructure safe. Penetration testers must understand the underlying infrastructure to identify potential security weaknesses.
- In a PaaS environment, the cloud provider is responsible[23] for securing the infrastructure, while the customer is responsible[23] for securing the applications running on top of the infrastructure. Penetration testers have to know how the configuration of the platform affects the security of the apps.
- In a SaaS environment, the cloud provider is responsible[23] for securing the entire stack, including the infrastructure, platform, and application. Penetration testers need to know how the service provider handles security and work with the service provider to make sure that testing doesn't interfere with the service.

The following are the key takeaways:

- The need for penetration testing of cloud assets and environments is essential.
- Understanding shared responsibility and how penetration testing fits into a Service Level Agreement[SLA] is essential for cloud security.

- An Overview of Penetration Testing Methods for Cloud-Based Services: Amazon Web Services (AWS), Microsoft Azure,[23] and Google Cloud Platform[23] (GCP).
- Identifying and understanding common cloud security threats(CST)[24] and vulnerabilities
- Understanding the common threats and vulnerabilities associated with cloud computing
- Optimum methodologies for conducting cloud penetration testing

Overall, it is important to understand the specific challenges and considerations associated with conducting penetration testing in each type of cloud environment in order to effectively identify and mitigate security risks.

3. METHODOLOGY

The article, "Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS[25] Environments," provides a comprehensive look at the methodology used to secure cloud application infrastructure. This article explores how penetration testing can be used[25] to identify weaknesses in cloud-based applications while also offering best practices for mitigating those vulnerabilities.

The authors begin by discussing the importance of understanding the different[26] types of clouds available and their associated risks. They then provide an overview of penetration testing techniques such as network scanning and vulnerability assessment that are commonly employed when conducting assessments in these environments. The authors also discuss various methods for hardening systems, including patching known flaws or deploying security controls like firewalls or encryption solutions. Finally, they offer guidance on developing policies around access control lists (ACLs) that can help organizations protect their data from malicious actors attempting to gain unauthorized access into networks or systems through misconfigurations in public-facing services such as APIs or web servers hosted within a given environment. Overall, this article provides a thorough examination of securing cloud application infrastructure using penetration testing methodologies, which is essential for any organization looking to move its operations onto these platforms with confidence in their security posture going forward. By providing detailed explanations about both common threats posed by utilizing certain types of[26] clouds and recommendations regarding mitigation strategies, this paper offers valuable insight into how organizations can ensure they remain secure while taking advantage of all that modern technology has to offer them today.

4. THE NEED FOR PENETRATION TESTING OF CLOUD ASSETS AND ENVIRONMENTS IS ESSENTIAL

Penetration testing is an essential part of any cloud asset and environment security strategy. And also, this test is an important step in ensuring the security of cloud assets and environments. As more organizations move their[1] operations to the cloud, the need for strong cybersecurity measures becomes increasingly important. It aids in identifying potential system flaws that malicious actors might exploit, enabling organizations to take proactive measures to reduce risks. Penetration testing involves simulating a cyberattack on a system[2] or network to find weaknesses and possible entry points for attackers. By simulating real-world attacks, penetration tests can help organizations figure out how their systems would respond to a real attack and come up with effective ways to stop it before it happens. Regards cloud assets and environments, penetration testing may help find any security risks that might come with using cloud resources. This is especially important because of how complex and changing cloud environments are,

where assets and infrastructure can be spread out and connected in many ways. Penetration testing is good for cloud assets and environments because it gives you a better idea of where the system might be weak and makes it easier to spot threats early on. Penetration testing also shows where more security measures may be needed, such as authentication protocols or access control policies that need to be tweaked or enforcement procedures that need to be tightened to protect against bad actors trying to get in without permission or steal data from inside the organization's network perimeter. Also, it can give useful information about which third-party services might need more thorough screening before they can be added to a company's existing infrastructure, since these services often have less strict security controls than internal resources. It's important to do penetration tests on cloud environments and assets often to stay safe and ahead of the curve. These tests can detect even minor vulnerabilities before they become a problem. It's important to find and fix security risks as soon as possible, before malicious attackers take advantage of them. This could cost a lot of money and hurt your reputation. As a result, all online businesses should strongly consider spending money on regular assessments to maintain a high level of cyber hygiene across the board and reduce risk exposure over time.

5. UNDERSTANDING SHARED RESPONSIBILITY AND HOW PENETRATION TESTING FITS INTO A SERVICE LEVEL AGREEMENT[SLA] IS ESSENTIAL FOR CLOUD SECURITY

Understanding shared responsibility is a key concept when it comes to cloud security. Shared responsibility means that both the cloud provider and the customer are responsible for maintaining secure systems. The provider takes on some of the burden, such as setting up infrastructure and providing access control measures, while customers must take steps to ensure their data remains safe from malicious actors or unauthorized access. This can include encrypting data at rest or in transit, using strong authentication methods, regularly patching software vulnerabilities, and following best practices[4] for user account management. Penetration testing is an important part of ensuring that a system meets its security requirements under this shared responsibility model. Penetration testing involves simulating attacks against a system in order to identify potential weaknesses before they can be exploited by attackers in real-life scenarios; this helps organizations determine what areas need improvement so they can better protect their assets from adversaries who may try to gain[4] unauthorized access or cause damage through malicious activities like malware injection or DDoS attacks. By performing regular penetration tests on their systems, either internally with tools available within an organization's IT resources or externally with specialized services provided by third-party companies, businesses will have greater confidence that their applications are robust enough against cyber threats. Ultimately, successful cloud security relies on working together between service providers and consumers. Additionally, performing regular penetration tests can also limit or eliminate any potential risks associated with this environment. In order to stay[3] on top of the ever-evolving technological landscape, companies must be vigilant and proactively manage any potential security risks. Investing in penetration testing is a great way to ensure your systems are secure and has numerous benefits for long-term success.

6. AN OVERVIEW OF PENETRATION TESTING APPROACHES FOR CLOUD-BASED SERVICES: AMAZON WEB SERVICES (AWS), MICROSOFT AZURE, AND GOOGLE CLOUD PLATFORM (GCP)

Penetration testing is a critical component of any cloud-based infrastructure. It helps organizations identify potential vulnerabilities in their systems[10] and take the necessary steps to mitigate them. As more

companies move to the cloud,[6] penetration testing has become increasingly important for ensuring security and compliance with various regulations. In this article, we will discuss how penetration testing can be approached on Amazon Web Services[6] (AWS), Microsoft Azure, and Google Cloud Platform[6] (GCP). When it comes to AWS, there are several tools available that allow users to perform automated vulnerability scans on their environment. These include Amazon Inspector, which checks how secure your system is; Trusted Advisor, which gives you detailed advice on how to best secure your resources; AWS Config Rules, which lets you set up rules based on industry standards like CIS Benchmarks; and Security Hub, which puts all your findings in one central dashboard so you can easily analyze and report on them. All of these services can help an organization see potential risks in their AWS environment so they can fix them quickly before they cause a breach or something else serious. Microsoft Azure customers looking for[7] ways to assess their environments' security postures should consider using its built-in threat detection service, called Azure Security Center (ASC). ASC uses machine learning algorithms that are designed to find malicious activity like brute force attacks or strange patterns of user behavior across many workloads hosted on the platform, such as virtual machines, databases, storage accounts, and so on. It also has advanced analytics features that give customers more information about threats to their systems and let them take action before damage is done. Last but not least, GCP has their own set of tools, such as the Cloud Security Scanner, Identity Aware Proxy (IAP), Access Transparency Logging (ATCL), etc., that could be used to do thorough assessments of customer environments. The first one lets scanning applications run inside GCP, and the second and third ones add more authentication and authorization layers, respectively. When all three technologies are used together, they provide complete coverage. This helps organizations[8] stay ahead of attackers by[9] constantly monitoring and detecting any suspicious activities happening inside the network perimeter. To summarize, penetration testing is a key component of protecting data assets from unauthorized access, manipulation, and misuse. However, each major cloud provider has a different set of solutions available depending upon customer requirements and budget constraints, so selecting the right tool mix becomes an essential part[9] of risk management strategy going forward.

7. IDENTIFYING AND UNDERSTANDING COMMON CLOUD SECURITY THREATS AND VULNERABILITIES

Cloud security threats and vulnerabilities are becoming increasingly important to understand as more businesses move their operations online. With the amount of data stored in cloud systems, it is essential that organizations take steps to protect themselves from potential attacks. This essay will discuss common cloud security threats(CST) and vulnerabilities, how they can be prevented, and why understanding them is so important for businesses today. The most common threat when using a cloud system is unauthorized access or malicious activity by an outside actor who gains access either through stolen credentials or exploiting vulnerable software configurations. Other risks include data breaches caused by improper configuration settings such as weak passwords; denial of service (DoS) attacks that overwhelm servers with requests; malware infections resulting from unpatched software programs; phishing scams aimed at stealing personal information; ransomware demands where hackers lock down systems until payment has been made; insider threats due to careless employees sharing sensitive information without proper authorization protocols in place, etc. To prevent these types of cyber-attacks, companies should implement multi-factor authentication measures, regularly update their system's software patches, use encryption technology for all stored data files and communications sent over the network, have strict policies governing employee usage and conduct on company networks, and deploy anti-virus protection solutions across all

devices used within the organization. Additionally, regular penetration testing should also be conducted on a routine basis to identify any existing weaknesses within your IT infrastructure before attackers can exploit them. Understanding these common cloud security threats(CST) and vulnerabilities is critical for any business operating online today because they could lead not only to financial losses but also to reputational damage if left unchecked or unprotected against malicious actors looking to gain access into corporate networks and steal confidential customer or company records. Taking proactive measures such as those mentioned above can help ensure that your business remains secure while still being able to operate efficiently without having to worry about potential issues arising due to unforeseen circumstances related to cybersecurity incidents occurring during the normal course of daily operations.

8. UNDERSTANDING THE COMMON THREATS AND VULNERABILITIES ASSOCIATED WITH CLOUD COMPUTING

Organizations that rely on cloud-based services should prioritize carrying out cloud penetration testing to identify any potential security vulnerabilities. This is an important element of risk management and crucial for protecting sensitive information. It helps to identify vulnerabilities in the system, allowing businesses to protect their data and infrastructure from malicious attacks. However, there are several challenges associated with cloud penetration testing[12] that can make it difficult for organizations to properly assess the security of their systems. One major challenge is identifying all of the assets within an organization's cloud environment. As more applications move into the cloud, it becomes increasingly difficult for companies to keep track of every asset they have deployed on various platforms and networks across multiple providers or regions. Without a comprehensive inventory list, it can be hard for testers to accurately assess potential threats or weaknesses in each component of an organization's digital landscape. Another problem with cloud penetration testing(CPT) is figuring out how to control access for different users or groups within a given system architecture. This includes both internal and external stakeholders, whose roles in an organization's network structure may require different levels of access. Additionally, many vendors do not provide detailed documentation regarding how user privileges are assigned, which makes assessing risk even more challenging. Organizations must also ensure compliance with industry regulations such as HIPAA when conducting any type of vulnerability assessment activity. Failure to adhere to these standards could result in costly fines if found noncompliant during audit reviews by regulators. A successful implementation requires an IT team to be organized and well-informed about the technology used in the organizational networks. This allows them to evaluate their systems properly while also protecting any confidential data. As cyber risks become more prevalent across businesses worldwide, protecting digital infrastructure has become critical. Cloud penetration testing(CPT) is a reliable approach to ensuring security and can be easily implemented in any organization.

9. OPTIMUM METHODOLOGIES FOR CONDUCTING CLOUD PENETRATION TESTING

Cloud penetration testing is a crucial part[13] of any organization's security strategy. It helps organizations identify and mitigate potential risks associated with the deployment of cloud-based applications, services, and infrastructure. To ensure that an organization's cloud environment is secure from malicious actors, best practices for cloud penetration testing must be followed. First and foremost, organizations should perform

regular assessments to determine their level of risk with regards to their existing security posture. This assessment should include identifying all assets within the system as well as evaluating how they are configured relative to industry standards or regulatory requirements such as HIPAA or PCI DSS compliance standards. Additionally, it is important that these assessments are conducted on a continuous basis so any new vulnerabilities can be identified quickly before they can cause harm to your systems or data integrity levels drop below acceptable thresholds due to misconfigurations over time. Organizations must have comprehensive logging capabilities in order to appropriately monitor activity within their system. This is essential for a successful system that can detect and respond to any suspicious activity. By having this visibility into user activities, IT teams will have better insight into what actions were taken during an attack attempt, which makes incident response much more efficient when responding quickly becomes necessary. Additionally, log files provide valuable information about who accessed what resources at specific times, which could prove invaluable if an investigation needs further evidence beyond just monitoring alerts triggered by suspicious behavior. When combined with other measures like encryption protocols for data privacy protection and access control policies restricting certain users from accessing sensitive information, cloud penetration tests become even more effective in helping keep your business safe from malicious actors looking for ways around traditional cyber defense mechanisms.

10. EXPLORING THE DIFFERENT SECURITY CHALLENGES FOR IAAS & PAAS

Cloud computing has changed the way businesses work by giving them a way to manage their IT infrastructure that is both cheap and effective. But with this new technology comes a higher risk of security threats that must be handled to protect data and systems from being hacked or accessed by people who shouldn't be able to. This article will talk about the different security problems that come with Infrastructure as a Service[13] (IaaS) and Platform as a Service[13] (PaaS) cloud applications. It will do this by talking about secure architecture design, securing virtual machines, and using containers on public clouds. Regards to protecting cloud applications from risks like data breaches or denial-of-service attacks, it's important to have a secure architecture design. Organizations should think about building encryption technologies like Transport Layer Security (TLS) and multi-factor authentication into their system designs and multi-factor authentication into their system designs to protect themselves as much as possible from these threats. Software configurations, which can provide[14] attackers with an easy entry point into networks if not properly managed. Securing virtual machines, which run multiple services at the same[14] time on one server instance, is another important part of protecting IaaS solutions. This makes them more vulnerable than physical servers, which can only run one application at a time. Organizations can better protect themselves from bad actors by putting firewalls between each machine in a cluster environment and updating the anti-virus programs on each VM instance on a regular basis. This keeps them safe from the new types of malware that are released online every day. Also, administrators should always keep track of user activity logs in VMs so that any suspicious actions can be caught quickly before more damage is done.

PaaS solutions that use containers require special attention as they don't have their own operating[14] systems, unlike virtual machines. Therefore, it is essential to ensure that these lightweight environments are adequately cared for. Containers do not generate their own resources but leverage those of the host[14] operating system. Due to this, they are more susceptible to attack from malicious actors who exploit the vulnerabilities of containers. So, organizations that use containerized workloads need to take extra steps to harden deployment images before putting them into production. This includes turning off features that aren't needed, like debugging mode, and adding extra layers of security through network segmentation and other

methods. These steps are meant to limit the number of points of exposure and possible intrusions that can happen during runtime operations. In conclusion, proper planning around secure[15] architecture design and taking proper precautions when dealing with both VMs and containers are key factors ensuring the robustness of cloud-based deployments, regardless of whether they use IaaS or PaaS models offered in today's marketplaces, thus allowing companies to reap the full benefits of modern-day distributed computing without having to worry[15] about it.

11. UNDERSTANDING THE PENETRATION TESTING CHALLENGES FOR SAAS APPLICATIONS

Penetration testing is an important part of ensuring the security of software-as-a-service (SaaS) applications. By proactively identifying[16] potential vulnerabilities and threats, organizations can mitigate the risk of data breaches or other malicious attacks. However, there are certain challenges associated with penetration testing[18] SaaS applications that must be addressed in order to ensure effective protection against cyber criminals. The first problem with penetration testing SaaS apps is figuring out how they are different from traditional on-premises systems. Since most SaaS solutions are hosted in the cloud, they might not have access to all the resources and tools that on-premises systems use to check for vulnerabilities and fix them. Due to complexity, such as multi-tenancy architectures or shared service models used by numerous customers at once, many organizations also lack visibility into their own infrastructure when evaluating mobile backend security. Because of this, these kinds of deployments need extra care during any kind of security evaluation process, like penetration tests, so that every possible threat vector can be found and dealt with before a system[17] or application update or patch release cycle goes live. Selecting the desired test cases for your company's SaaS apps are one of the few main challenges when performing a successful penetration test. It's important to[18] ensure that those tests meet your organization's specific needs. For example, if you're specifically looking for authentication issues, you should focus your efforts, accordingly, using automated tools where available, rather than trying to cover too much ground, which could lead to potentially missing critical findings. It also helps if testers understand common attack vectors used against web apps so they know what types of scenarios might need further investigation during their assessment activities. All this said, having an experienced team that understands the technology stack being tested well enough to develop custom scripts tailored towards uncovering any weaknesses present within a particular environment will ultimately yield the best results overall in terms of the time spent[18] conducting those tests themselves.

12. IDENTIFYING AND SECURING VULNERABILITIES IN CLOUD APPLICATIONS

Cloud-based applications are becoming increasingly prevalent in modern businesses as they enable remote data access from any location and at any time. Even though cloud services provide immense convenience and flexibility, they also bring with them potential security threats. To ensure the safety of sensitive information, measures must be taken to mitigate these risks effectively. Identifying potential vulnerabilities in a cloud application is an essential step for ensuring the safety of data stored on the platform. The best way to find potential weaknesses is with a full vulnerability assessment program that includes regular scans and tests done by experts who know what threats are out there right now. The assessments should focus on identifying both known and unknown weaknesses that may exist within the system architecture or codebase itself. Once problems are found, it's important to find ways to fix them. Depending on how bad the problems are, this could mean fixing existing flaws or adding extra security measures like encryption or two-factor authentication systems. Additionally, organizations can consider adopting the principles of the zero-trust

model for better protection against unauthorized access attempts. After addressing the potential risks associated with cloud applications and putting in place measures to protect them, businesses should regularly scan their environments for any suspicious activity. This way, they can stay one[19] step ahead of any malicious actors. This will help them stay ahead of emerging cyberattacks while providing continuous assurance about operational integrity and resilience across their digital infrastructure. To sum it up, the right authentication and security measures help secure any AI-powered applications deployed on public or private clouds while still preserving customer privacy.

13. THE UNIQUE CHALLENGES OF PENETRATION TESTING ON CLOUD-BASED APPLICATIONS

Penetration testing is an essential part of any organization's security strategy. It helps identify and address vulnerabilities in applications, networks, systems, and other IT components. However, when it comes to cloud-based applications, there are unique challenges that must be addressed. First is the complexity of the environment itself. Cloud-based applications often run on Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) environments, which can make it hard for penetration testers to get access to all the areas they need to test. Also, these environments may have different levels of control over how data is stored, which makes it harder to test different attack scenarios, like SQL injection attacks or cross-site scripting attempts, without risking that customer data will be compromised during tests done by outside parties, like penetration testers, and cause service to be interrupted. Finally, there are also compliance regulations that need to be taken into consideration when conducting penetration tests on IaaS, PaaS, and SaaS environments, such as GDPR, which requires organizations to not only protect their customers' personal information but also ensure third-party contractors follow strict rules regarding how they handle this type of confidential information while performing services like vulnerability assessments and pen tests on their behalf; failure to do so could result in severe penalties from regulatory bodies if found out after audits take place at later stages down the line. Therefore, it's important for both internal teams responsible for application security within organizations and external vendors providing these services to understand the unique challenges associated with cloud-based application testing before starting any activity-related pen test campaigns against them.

14. CONCLUSIONS

Cloud computing has become increasingly popular for businesses of all sizes, as it offers a range of advantages such as scalability, agility and cost savings. However, with the increased adoption of cloud services comes an increase in security risks that can be difficult to manage without proper penetration testing. Penetration testing[20] is a process used to identify vulnerabilities and security flaws within cloud applications and infrastructure. It allows organizations to better understand their environment's attack surface by simulating real-world attacks on the system using automated tools or manual techniques.

When conducting penetration tests on IaaS/PaaS/SaaS environments there are several challenges that must be taken into account including understanding shared responsibility between provider and customer when it comes to securing data; understanding how different providers have differing approaches towards securing their assets; being aware of common threats specific for each platform like AWS, Azure or GCP; having knowledge about current best practices regarding cloud architecture design principles; being able detect any misconfigurations in networks or systems which could lead attackers bypassing authentication mechanisms etc.. Additionally one should consider performing periodic vulnerability scans even after successful completion of initial pentesting phase since new vulnerabilities may appear over time due

changing conditions (e.g., software updates). Summarize, having a secure architecture plan and taking the necessary precautions when dealing with virtual machines and containers can help ensure successful cloud-based deployments no matter if an infrastructure as a service (IaaS) or platform as a service[20] (PaaS) model is being used. Companies can reap the full benefits of modern distributed computing without having to worry about the technical aspects due to their high scalability and agility.

To sum up - while there are many benefits associated with utilizing Cloud Services they also present unique challenges when attempting secure them properly via Pentesting activities . Therefore , organizations should take into consideration various factors before engaging in such activity – from analyzing shared responsibility[20] model between provider & customer , assessing existing threat landscape & following industry best practices . This will ensure continuous protection against malicious actors targeting vulnerable components within Cloud Infrastructure. Penetration testing is no longer something that companies can do without. It is now a requirement for organizations to ensure the safety and security of their systems and networks. Carrying out these tests can help strengthen an organization's security stance. Various regulations now require businesses and organizations to check their technical infrastructure regularly. This helps ensure that everything is working properly and securely. Doing so can also help address any potential issues quickly and efficiently. It is usually better to hire an external service provider for a penetration test as an internal team could have prior knowledge of your cloud presence, which could lead to certain details being overlooked. For more information, you can set up a call with the provider. In summary, it is clear that utilizing both ethical hacking[22] and penetration testing are essential components when it comes to ensuring proper cloud application safety. Not only do they help identify weaknesses within existing infrastructure, but they also enable companies to create more comprehensive plans for mitigating risks associated with virtual operations going forward. As such, understanding how to best utilize each technique should remain a top priority moving forward given its critical role in safeguarding customer information assets against external threats.

ACKNOWLEDGEMENT

This research did not rely on external funding and was self-funded by the authors, who declared no conflicts of interest.

REFERENCES

[1] The Future of Global Outsourcing: Trends and Predictions for 2023 and Beyond. (2023, March 9). Sourcefit BPO Philippines: Custom Offshore Staffing Solutions.
[2] Guidepointsecurity.com. (n.d.). https://www.guidepointsecurity.com/education-center/cloud-penetration-testing/.
[3] 03- Penetration Testing Quiz Flashcards by James McCarter | Brainscape. (n.d.).
[4] Cynet. (2023, January 6). Unauthorized Access: 5 Best Practices to Avoid Data Breaches.
[5] Taylor, C. (2021, January 28). Cloud Computing and Service Level Agreements (SLAs) | Datamation. Datamation.
[6] E. (2023, January 10). The Complete Guide to Becoming a Certified Cloud Security Professional. Cybersecurity Exchange.
[7] T. (2023b, March 10). Azure threat protection. Microsoft Learn. https://learn.microsoft.com/en-us/azure/security/fundamentals/threat-detection
[8] Ajimal, A. (2023, January 18). How continuous data monitoring helps organizations. Nowigence Inc.
[9] Bellekens, X. (2023, January 30). What are Cyber Threat Intelligence Feeds ? Lupovis.
[10] Tagade, K. (2022, April 25). NIST Penetration Testing:Guide,Framework and How to Achieve Security Compliance. Astra Security Blog.

[11] Team, N. (2022, February 1). Top 10 Cloud Security Threats. IT Solutions, IT Service Company in Long Island.
[12] S. (2023b, March 4). Cloud Penetration Testing From The Field. CyberDome.
[13] What is Cloud Penetration Testing? | CSA. (2022, February 12).
[14] Team, D. (2018, November 29). Infrastructure as a Service (IaaS) – Working, Example, Benefits. DataFlair.
[15] Cure, A. (2015, February 5). C#/.NET/Core Training in Denver, CO – May 2019.
[16] Dr. A.SHAJI GEORGE, & A.S.HOVAN GEORGE. (2022). Potential Risk: Hosting Cloud Services Outside the Country. International Journal of Advanced Research in Computer and Communication Engineering, 11(4), 5–11. https://doi.org/10.5281/zenodo.6548114
[17] Spring, M. (2023, March 9). Cybersecurity Best Practices for MSPs in 2023. Evolved Office.
[18] Author, V., & Author, V. (2021, June 29). SaaS application pentest: What main security challenges? VAADATA - Ethical Hacking Services.
[19] How CISOs can stay one step ahead of 2023's risks, threats and attacks. (2023, January 1). CB ISO News.
[20] Cybersecurity penetration testing explained: what is pen testing? (2023, March 8).
[21] Testgrid, Y. (2023, February 18). The Cloud Penetration Testing Handbook : TestGrid. TestGrid | Blog.
[22] E. (2023b, March 6). What's the Difference Between Ethical Hacking and Penetration Testing? Cybersecurity Exchange.
[23] Grier, S. (2020, September 25). The cloud shared responsibility model for IaaS, PaaS and SaaS. Cloud Computing.
[24] [24] Fichtner, E. (2022, March 9). The Most Common Cloud Security Threats and How to Avoid Them. Datto.
[25] McPherson, W., Tang, A., & Mulholland, I. (2019, July 11). Ensure Cloud Security in IaaS, PaaS, and SaaS Environments. Info-Tech Research Group.
[26] Student Project: The Types of Clouds and What They Mean | NASA/JPL Edu. (2021, May 26). NASA/JPL Edu.