5-5-2022

Compliance Based Penetration Testing as a Service

Srinivasulu Vuggumudi
Dakota State University, srvuggumudi@pluto.dsu.edu

Kaushik Ragothaman
Dakota State University, kaushik.muthusamyragothaman@trojans.dsu.edu

Yong Wang
Dakota State University, yong.wang@dsu.edu

Compliance Based Penetration Testing as a Service

Srinivasulu Vuggumudi
Dakota State University
srvuggumudi@pluto.dsu.edu

Kaushik Ragothaman
Dakota State University
kaushik.muthusamyragothaman@trojans.dsu.edu

Yong Wang
Dakota State University
yong.wang@dsu.edu

ABSTRACT

The current penetration testing method practiced in the information systems domain is insufficient to protect information systems. Penetration testing is part of the final acceptance criteria before the system is released into a production environment. Once the system is in production, the environment and configuration are bound to change for various reasons, especially in cloud environments. This change can create vulnerabilities, and hackers take advantage of them. In cloud service models like PaaS, security is a shared responsibility of tenant and provider, and it is challenging to perform penetration testing. This paper introduces a new method called Compliance Based Penetration Testing (CBPT). The CBPT method explicitly targets PaaS environments to identify critical issues in cloud-based environments. As the cloud is the way moving forward, this approach will be beneficial and save effort and cost for all cloud consumers.

Keywords

Penetration Testing; Compliance Based Penetration Testing; CBPT; PaaS.

INTRODUCTION

The cyber landscape is becoming increasingly complex; cyber-attacks are one of the major challenges for corporations. The number of cyber-attacks is exploding day by day, shaking even the powerful countries. Penetration testing is an expensive process. Hence, it is performed at the end of the system development, when a significant milestone is reached, and periodically to fulfill compliance requirements when the system is in a production environment. Typically, corporations perform penetration testing at least once a year, but the system and network's critical components may be tested more frequently every six months (Botenau 2011).

"Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network." (Scarfone et al. 2008). Generally, penetration testers focus on the network, operating system, and application to derive test cases. Once an information system is in a production environment, the system environment and configuration are bound to change for various reasons, especially in cloud environments. The changes in environment and configuration can create new vulnerabilities, and they cannot be discovered until the next penetration test. There is a high probability that hackers can exploit vulnerabilities between penetration tests. There is a solid need to solve the challenge of avoiding the exploitation of vulnerabilities between the tests. This paper introduces the Compliance Based Penetration Testing (CBPT) method to prevent the exploitation of vulnerabilities between penetration tests. The CBPT method takes compliance as the base. Meeting compliance requirements does not guarantee security (Grossman 2008). However, it serves as a baseline to build security. The CBPT method also facilitates adding any security test case outside of compliance standards a customer thinks is required. In the context of CBPT, compliance includes regulatory standards like PCI-DSS, HIPAA, GDPR, etc., and corporate security standards (which vary from corporation to corporation). It is an automated method to help both the cloud service providers and customers. This research is focused on enhancing penetration testing in a Platform as a Service (PaaS) environment.

LITERATURE REVIEW

We performed an extensive search for existing academic literature. But we couldn't find relevant articles that performed penetration testing based on test cases extracted from compliance requirements or PaaS environments. However, systematic reviews on penetration testing exist. Bertoglio et al. stressed the need for more discussion on security testing scenarios in cloud computing environments (Dalalana Bertoglio and Zorzo 2017). Leszczyna et al. reviewed cybersecurity assessment methods.

They found that all the checklist-based and compliance checking methods obtain the cumulative value of the security level of an entire system (Leszczyna 2021). Tiwari et al. state that there is a security gap between the application or host security and network security in PaaS environments. They state that it is beyond the scope of the service providers and mention the need for PaaS providers to ensure access to ready-to-use features for their customers to assess application-level security (Tiwari et al., 2021). Many vendors like SysDig (Sysdig n.d.), Tenable (Tenable n.d.), Netskope (Netskope n.d.), Qualys (Qualys n.d.), etc., provide compliance verification and vulnerability scanning solutions. These commercial solutions typically scan the hosts present in the cloud environment for misconfiguration, suspicious activity, etc., and report the findings based on a predefined set of controls to ensure compliance. It is almost an automated checklist approach. A user may customize the controls but not have the option to upload and verify their test cases. In addition, the commercial tools do not perform penetration testing.

We consider the scope for further research to ensure compliance in cloud environments, the need for ready-to-use features in PaaS, and the shortcomings of existing commercial solutions to propose our CBPT approach, which is based on compliance standards, automated, and facilitates the inclusion of user-defined test cases for penetration testing.

RESEARCH METHODOLOGY

Design Science (DS) research methodology is selected to solve the problem with the current penetration methods prevalent in the information technology industry. The proposed research study follows the seven guidelines suggested by Hevner et al. in design science research (Hevner et al. 2004). The results from each guideline are: 1) The artifact in this research study is a method called Compliance Based Penetration Testing (CBPT). 2) It is designed to solve the problem of exploiting vulnerabilities between penetration tests. 3) It will be evaluated with the case study method. 4) CBPT is a new penetration testing method contributing to the research. 5) The artifact is designed based on the theory behind penetration testing, Platform as a Service, and identified potential gaps in the literature on what needs to be done to enhance penetration testing. 6) The researchers reviewed and modified the design several times. In this process, we identified the benefits of adding a vulnerability scanner and file integrity checker to the CBPT process. Similarly, corporate security requirements are also added to the compliance requirements. 7) The proposed method motivates technical and managerial audiences to reap the benefits of complementing regular penetration testing with CBPT. It is a great motivation for management because CBPT is an automated process and is cost-effective.

PROPOSED METHOD – COMPLIANCE-BASED PENETRATION TESTING (CBPT)

In the proposed CBPT method, PaaS providers provide an option to select the required compliance like HIPAA, PCI-DSS, etc., when provisioning the host to a customer. Customers will be prompted to accept the installation of an agent program to monitor the host's compliance and an option to share test cases based on their corporate security requirements. It is the customers' choice to accept the installation of the agent program or not. They get a massive benefit of compliance monitoring daily or needed basis. The service provider runs Compliance Verifier and Manager (CVM) program at the hypervisor level so that it can communicate with agents on all the instances hosted in the hypervisor environment.

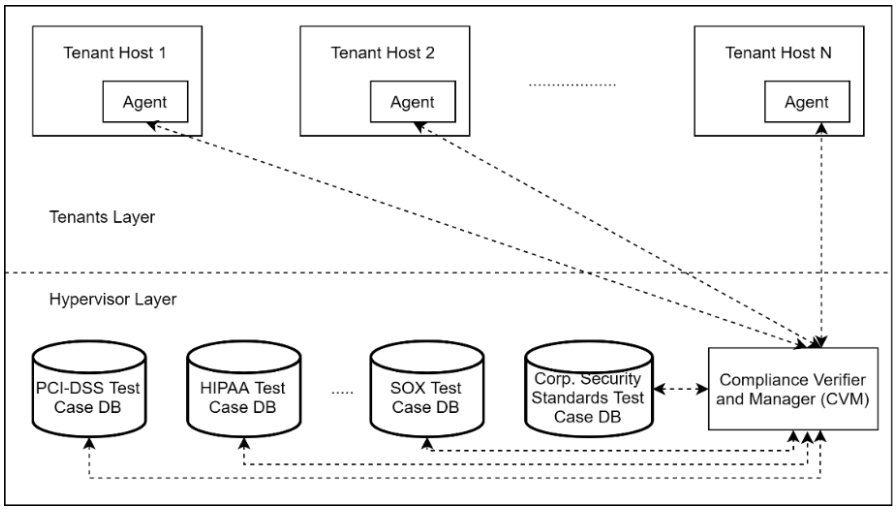

Figure 1 - PaaS Environment Equipped with CBPT

As shown in Figure 1, the Compliance Verifier and Manager (CVM) will access databases containing test cases based on the compliance standards. The agents on each hosted instance communicate with CVM and request a penetration test daily based

on the time set by the customer. Customers will also have the option to request penetration tests whenever a significant change is made to the host environment. CVM runs penetration tests based on compliance and corporate security standards of the customer. At the hypervisor level, the test case databases will be available for each compliance standard. Each compliance standard, like PCI-DSS, HIPPA, SOX, etc., provides guidelines regarding how the network, access, authorization, and privacy configurations need to be maintained to comply with the respective standard. The test cases for CBPT will be derived from those guidelines set by the respective compliance standards and saved in the test case database.

CVM pulls CBPT test cases from the test case database and runs automated penetration tests created by the service provider. After the CBPT tests are run, CVM also runs a file integrity checker and vulnerability scanner. A vulnerability scanner identifies possible vulnerabilities based on service banners and network responses (Northcutt et al. 2006). The file integrity checker computes the hash value of the system files present in a host to verify them against unauthorized changes or misconfigurations. The vulnerability scanner and file integrity checker complements the CBPT. Finally, CVM compiles a CBPT test report, file integrity checker report, and vulnerability scanner results and sends an email to the tenant's compliance team. If any CBPT test case fails, the alert will be delivered to the tenant's compliance team members. Failure of a CBPT test case means a security vulnerability is created due to changes in the tenant host's environment configuration. CVM maintains stores reports of each tenant in a database to analyze vulnerability discovery trends.

PROPOSED EVALUATION

We plan to evaluate our proposed CBPT method using the case study method. For our case study, we select two customers (customer A and customer B) of similar size in the same line of business, use cloud infrastructure with the same service provider, and perform manual penetration testing every six months. We let customer A use the CBPT artifact and remediate the vulnerabilities, if any, as soon as CBPT reports them. We let CBPT service run for six months with customer A. We stop CBPT service as soon as both customer A and customer B gets ready for manual penetration testing the second time. Once both customers complete the testing, we collect their test reports. We expect to see fewer vulnerability findings with customer A compared with customer B. The reason is customer A would be addressing the vulnerabilities as soon as CBPT reports, but customer B waited six months without performing penetration tests and had no CBPT service implemented.

CONCLUSION

This paper illustrated the limitations of the current penetration testing methods prevalent in the information systems domain. A new approach to performing penetration testing is proposed, compliance-based penetration testing (CBPT). Since security is a shared responsibility of tenant and provider, the goal of CBPT is to complement the current penetration testing method in the information systems domain. The test cases derived from the technology-related requirements are enough to achieve the goal of CBPT, i.e., providing baseline security required by respective compliance standards.

REFERENCES

1. Botenau, D. 2011. "Penetration Testing: Hacking Made Ethical to Test System Security," *Canadian Manager* (36:3), pp. 10–11.
2. Dalalana Bertoglio, D., and Zorzo, A. F. 2017. "Overview and Open Issues on Penetration Test," *Journal of the Brazilian Computer Society* (23:1), p. 2. (https://doi.org/10.1186/s13173-017-0051-1).
3. Grossman, W. M. 2008. "Complying to a False Sense of Security," *Infosecurity* (5:7), pp. 24–27. (https://doi.org/https://doi.org/10.1016/S1754-4548(08)70122-0).
4. Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly*, JSTOR, pp. 75–105.
5. Leszczyna, R. 2021. "Review of Cybersecurity Assessment Methods: Applicability Perspective," *Computers & Security* (108), p. 102376. (https://doi.org/https://doi.org/10.1016/j.cose.2021.102376).
6. Netskope. (n.d.). "Maintain Cloud Compliance - Netskope." (https://www.netskope.com/solutions/compliance, accessed July 3, 2022).
7. Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Siles, R., and Mancini, S. 2006. "Penetration Testing: Assessing Your Overall Security before Attackers Do," *Sponsored by Core Impact, SANS Analyst Program* (3:6), p. 22.
8. Qualys. (n.d.). "Qualys Cloud Security Assessment." (https://www.qualys.com/apps/cloud-security-assessment/, accessed July 3, 2022).
9. Scarfone, K., Souppaya, M., Cody, A., and Orebaugh, A. 2008. "Technical Guide to Information Security Testing and Assessment." (https://csrc.nist.gov/publications/detail/sp/800-115/final).
10. Sysdig. (n.d.). "Cloud and Container Compliance - Sysdig." (https://sysdig.com/products/secure/cloud-and-container-compliance/).

11. Tenable. (n.d.). "Compliance | Tenable." (https://www.tenable.com/solutions/compliance).
12. Tiwari, A., Patel, P., and Sharma, D. 2021. "Vulnerability Assessment and Penetration Testing Approach Towards Cloud-Based Application and Related Services," *International Journal of Scientific Research in Science, Engineering and Technology*, pp. 395–403. (https://doi.org/10.32628/IJSRSET218346).