# Cloud Penetration Testing

**Denisa-Nicoleta MIHALACHE**
Faculty of Electronics, Telecommunications, and Information Technology, National University of Science and Technology POLITEHNICA Bucharest, Romania
denisa.mihalache@stud.etti.upb.ro

**Abstract**

*The utilization of cloud computing has been growing exponentially, becoming the preferred platform for businesses of all sizes, from start-ups to large corporations. However, this shift towards cloud computing brought about the responsibility to ensure the security of cloud applications and data from malicious attacks. The joint responsibility model of cloud security requires both service providers and businesses to maintain security. Identity and access management are shared responsibility models, requiring protocols and ethical hacking to ensure data protection. Advanced security measures like penetration testing are essential to establish a secure virtual environment. The primary aim of this research paper is to demonstrate how important penetration testing is for an organization even with security features that cloud providers implemented.*

**Index terms:** cyber-attacks, cloud infrastructure, cloud penetration testing, cloud security, zero-trust model

## References

[1]. RedHat, (2022, August 16), "IaaS vs. PaaS vs. SaaS," Available: https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas.

[2]. Grier, S. (2020, September 25), "The cloud shared responsibility model for IaaS, PaaSand SaaS. Cloud Computing".

[3]. Microsoft, "Describe Software as a Service," Available: https://learn.microsoft.com/ro-ro/training/modules/describe-cloud-service-types/4-describe-software-service.

[4]. Microsoft, "Describe the shared responsibility model," Available: https://learn.microsoft.com/ro-ro/training/modules/describe-cloud-compute/4-describe-shared-responsibility-model?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.microsoft-azure-fundamentals-describe-cloud-concepts.

[5]. Microsoft, "Embrace proactive security with Zero Trust", Available: https://www.microsoft.com/en-us/security/business/zero-trust.

[6]. S. Vankirk, "The Complete Guide to Becoming a Certified Cloud Security Professional." Available: https://www.eccouncil.org/cybersecurity-exchange/cloud-security/about-certified-cloud-security-professionals/.
[7]. Guru99, "Google Cloud vs AWS: Differences Between AWS and GCP," Available: https://www.guru99.com/google-cloud-vs-aws.html.
[8]. Microsoft Learn, "Azure threat protection," Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/threat-detection.
[9]. Bellekens, X. (2023, January 30). "What are Cyber Threat Intelligence Feeds?," Available: https://www.lupovis.io/what-are-cyber-threat-intelligence-feeds/.
[10]. Cobalt, "Azure AD: Pentesting Fundamentals", Available: https://www.cobalt.io/blog/azure-ad-pentesting-fundamentals.
[11]. GitHub, "Azure Active Directory", Available: https://github.com/rootsecdev/Azure-Red-Team#password-spray.
[12]. Zigmax, "AAD | Password Spray Attack", Available: https://zigmax.net/aad-password-spray-attack/.
[13]. Derk van der Woude (2021, May 24), "Azure AD Password spray; from attack to detection (and prevention)" Available: https://derkvanderwoude.medium.com/password-spray-from-attack-to-detection-and-prevention-87c48cede0c0.
[14]. GitHub, "ROADtools", Available: https://github.com/dirkjanm/ROADtools.
[15]. Imperva, "Penetration Testing", Available: https://www.imperva.com/learn/application-security/penetration-testing/.