Cloud Penetration Testing for Red Teamers : Learn How to Effectively Pentest AWS, Azure, and GCP Applications /

Crawley, Kim,
author

Monografía

Get to grips with cloud exploits, learn the fundamentals of cloud security, and secure your organization's network by pentesting AWS, Azure, and GCP effectively Key Features Discover how enterprises use AWS, Azure, and GCP as well as the applications and services unique to each platform Understand the key principles of successful pentesting and its application to cloud networks, DevOps, and containerized networks (Docker and Kubernetes) Get acquainted with the penetration testing tools and security measures specific to each platform Purchase of the print or Kindle book includes a free PDF eBook Book Description With AWS, Azure, and GCP gaining prominence, mastering their unique features, ecosystems, and penetration testing protocols has become an indispensable skill, which is precisely what this pentesting guide for cloud platforms will help you achieve. As you navigate through the chapters, you'll explore the intricacies of cloud security testing and gain valuable insights into how pentesters and red teamers evaluate cloud environments effectively. In addition to its coverage of these cloud platforms, the book also guides you through modern methodologies for testing containerization technologies such as Docker and Kubernetes, which are fast becoming staples in the cloud ecosystem. Additionally, it places extended focus on penetration testing AWS, Azure, and GCP through serverless applications and specialized tools. These sections will equip you with the tactics and tools necessary to exploit vulnerabilities specific to serverless architecture, thus providing a more rounded skill set. By the end of this cloud security book, you'll not only have a comprehensive understanding of the standard approaches to cloud penetration testing but will also be proficient in identifying and mitigating vulnerabilities that are unique to cloud environments. What you will learn Familiarize yourself with the evolution of cloud networks Navigate and secure complex environments that use more than one cloud service Conduct vulnerability assessments to identify weak points in cloud configurations Secure your cloud infrastructure by learning about common cyber attack techniques Explore various strategies to successfully counter complex cloud attacks Delve into the most common AWS, Azure, and GCP services and their applications for businesses Understand the collaboration between red teamers, cloud administrators, and other stakeholders for cloud pentesting Who this book is for This book is for pentesters, aspiring pentesters, and red team members seeking specialized skills for leading cloud platforms--AWS, Azure, and GCP. Those working in defensive security roles will also find this book useful to extend their cloud security skills

https://rebiunoda.pro.baratznet.cloud:28443/OpacDiscovery/public/catalog/detail/b2FpOmNlbGVicmF0aW9uOmVzLmJhcmF0ei5yZW4vMzQ0Njc0MjE

Título: Cloud Penetration Testing for Red Teamers Learn How to Effectively Pentest AWS, Azure, and GCP Applications Kim Crawley

Edición: 1st ed

Editorial: Birmingham, England Packt Publishing Ltd. [2023] 2023

Descripción física: 1 online resource (298 pages)

Nota general: Includes index

Contenido: Cover -- Title Page -- Copyright -- Dedication -- Contributors -- Table of Contents -- Preface -- Part 1: Today's Cloud Networks and Their Security Implications -- Chapter 1: How Do Enterprises Utilize and Implement Cloud Networks? -- Cloud networks today -- Hybrid cloud, all-cloud, and multi-cloud networks -- All-cloud networks -- Hybrid cloud networks -- Multi-cloud networks -- Why an organization would have a multi-cloud network -- The cloud migration process -- Security responsibilities in the cloud -- AWS -- Azure -- GCP -- The difference between IaaS, PaaS, and SaaS -- Summary -- Further reading -- Chapter 2: How Are Cloud Networks Cyber Attacked? -- Understanding penetration testing -- External and internal attacks -- External cyberattacks -- Internal cyberattacks -- Attacks on the confidentiality, integrity, and availability of cloud data -- Confidentiality -- Integrity -- Availability -- Understanding lateral movement in the cloud -- Exploitation of remote services -- Internal spearphishing -- Lateral tool transfer -- Remote service session hijacking -- Software deployment tools -- Tainted shared content -- Zero-trust networks -- Summary -- Further reading -- Chapter 3: Key Concepts for Pentesting Today's Cloud Networks -- Cloud platform policies, benchmark checks, and services enumeration -- Exposed services, permissions, and integrations -- Exposed services -- Permissions -- Cloud integration -- CVE, CVSS, and vulnerabilities -- Vulnerabilities -- The MITRE database -- How do vulnerabilities get recorded in the CVE database? -- Purple teaming and writing pentest reports -- Purple teaming -- Writing pentest reports -- Summary -- Further reading -- Part 2: Pentesting AWS -- Chapter 4: Security Features in AWS -- Introduction to AWS -- Frequently used AWS SaaS features -- AWS IaaS features -- Compute services -- Storage services AWS PaaS features -- AWS security controls and tools -- Security controls -- Security tools -- Summary -- Further reading -- Chapter 5: Pentesting AWS Features through Serverless Applications and Tools -- Technical requirements -- How to get an AWS network -- Using AWS PowerShell and the AWS CLI -- Bash commands -- PowerShell commands -- Exploring AWS-native security tools -- AWS Security Hub -- Amazon Inspector -- Installing and preparing AWS pentesting tools -- Prowler -- Pacu -- Cred Scanner -- CloudFrunt -- Redboto -- Exploiting AWS applications -- Prowler -- Pacu -- Summary -- Further reading -- Chapter 6: Pentesting Containerized Applications in AWS -- Technical requirements -- How containerization works -- How Docker works in AWS -- Installing a Docker cluster in AWS with Amazon ECS -- Deploying Docker with Docker Desktop -- How Kubernetes works in AWS -- Docker and Kubernetes pentesting techniques in AWS -- Installation in Docker -- Installation in Kubernetes -- Summary -- Further reading -- Part 3: Pentesting Microsoft Azure -- Chapter 7: Security Features in Azure -- Introduction to Azure -- Frequently used Azure SaaS applications -- Azure Maps -- Azure Digital Twins -- Azure Monitor -- Microsoft Cost Management -- Azure Advisor -- Network Watcher -- Azure IaaS applications -- Azure Virtual Machines -- Azure Kubernetes Service -- Azure Container Instances -- Azure Dedicated Host -- Azure PaaS applications -- Azure SQL Database -- Web Apps -- Mobile Apps -- Azure Logic Apps -- Azure Functions -- Azure security controls and tools -- Security controls -- Security tools -- Summary -- Further reading -- Chapter 8: Pentesting Azure Features through Serverless Applications and Tools -- Technical requirements -- Setting up an Azure instance -- Setting up an Azure account -- Using Azure Cloud Shell and PowerShell -- Azure native security tools Microsoft Defender -- Azure pentesting tools -- Prowler -- MFASweep -- ScoutSuite -- Exploiting Azure applications -- Prowler -- MFASweep -- ScoutSuite -- Summary -- Further reading -- Chapter 9: Pentesting Containerized Applications in Azure -- Technical requirements -- How containerization works -- How Docker works in Azure -- How Kubernetes works in Azure -- Docker and Kubernetes pentesting techniques in Azure -- kube-hunter -- kdigger -- Summary -- Further reading -- Part 4: Pentesting GCP -- Chapter 10: Security Features in GCP -- Introduction to GCP -- Frequently used GCP SaaS applications -- Google Workspace -- Google App Engine -- Cost Management -- Google Cloud app -- Google Marketing Platform -- GCP IaaS services -- Compute Engine -- Cloud Storage -- Shielded VMs -- Sole-tenant nodes -- GCP PaaS services -- Cloud SDK -- Cloud SQL -- Cloud Run -- GKE -- Anthos -- GCP security controls and tools -- Security controls -- Security tools -- Summary -- Further reading -- Chapter 11: Pentesting GCP Features through Serverless Applications and Tools -- Technical requirements -- GCP free tier -- Launching a GCP

ISBN: 1-80324-886-6

Materia: Informática en la nube- Security measures Informática en la nube- Testing Computer security

Enlace a formato físico adicional: 9781803248486