Cloud PenTest - AWS and Azure by Joas

Azure Security
- https://github.com/LennonCMJ/pentest_script/blob/master/Azure_Testing.md
- https://github.com/dafthack/CloudPentestCheatsheets
- https://github.com/mattrotlevi/lava
- https://github.com/Azure/Azure-Security-Center
- https://github.com/kmcquade/awesome-azure-security
- https://github.com/MicrosoftLearning/AZ-500-Azure-Security
- https://github.com/Azure/Azure-Network-Security
- https://github.com/MicrosoftDocs/SecurityBenchmarks
- https://microsoftlearning.github.io/AZ500-AzureSecurityTechnologies/
- https://www.cisecurity.org/benchmark/azure/

PenTest in Azure
- Enumeration
  - o365creeper - Enumerate valid email addresses
  - CloudBrute - Tool to find a cloud infrastructure of a company on top Cloud providers
  - cloud_enum - Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud
  - Azucar - Security auditing tool for Azure environments
  - CrowdStrike Reporting Tool for Azure (CRT) - Query Azure AD/O365 tenants for hard to find permissions and configuration settings
  - ScoutSuite - Multi-cloud security auditing tool. Security posture assessment of different cloud environments.
  - BlobHunter - A tool for scanning Azure blob storage accounts for publicly opened blobs
  - Grayhat Warfare - Open Azure blobs and AWS bucket search
- Information Gathering
  - o365recon - Information gathering with valid credentials to Azure
  - Get-MsolRolesAndMembers.ps1 - Retrieve list of roles and associated role members
  - ROADtools - Framework to interact with Azure AD
  - PowerZure - PowerShell framework to assess Azure security
  - Azurite - Enumeration and reconnaissance activities in the Microsoft Azure Cloud
  - Sparrow.ps1 - Helps to detect possible compromised accounts and applications in the Azure/M365 environment
  - Hawk - Powershell based tool for gathering information related to O365 intrusions and potential breaches
  - Microsoft Azure AD Assessment - Tooling for assessing an Azure AD tenant state and configuration
- Lateral Movement
  - Stormspotter - Azure Red Team tool for graphing Azure and Azure Active Directory objects
  - AzureADLateralMovement - Lateral Movement graph for Azure Active Directory
  - SkyArk - Discover, assess and secure the most privileged entities in Azure and AWS
- Exploitation
  - MicroBurst - A collection of scripts for assessing Microsoft Azure security
  - azuread_decrypt_msol_v2.ps1 - Decrypt Azure AD MSOL service account
  - Credential Attacks
    - MSOLSpray - A password spraying tool for Microsoft Online accounts (Azure/O365)
    - MFASweep - A tool for checking if MFA is enabled on multiple Microsoft Services Resources
    - adconnectdump - Dump Azure AD Connect credentials for Azure AD and Active Directory
- Abusing Azure AD SSO with the Primary Refresh Token
- Abusing dynamic groups in Azure AD for Privilege Escalation
- Attacking Azure, Azure AD, and Introducing PowerZure
- Attacking Azure & Azure AD, Part II
- Azure AD Connect for Red Teamers
- Azure AD Introduction for Red Teamers
- Azure AD Pass The Certificate
- Azure AD privilege escalation - Taking over default application permissions as Application Admin
- Defense and Detection for Attacks Within Azure
- Hunting Azure Admins for Vertical Escalation
- Impersonating Office 365 Users With Mimikatz
- Lateral Movement from Azure to On-Prem AD
- Malicious Azure AD Application Registrations
- Moving laterally between Azure AD joined machines
- CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory
- Privilege Escalation Vulnerability in Azure Functions
- Azure Application Proxy C2
- Recovering Plaintext Passwords from Azure Virtual Machines like It's the 1990s
- Azure Articles from NetSPI
- Azure Cheat Sheet on CloudSecDocs
- Resources about Azure from Cloudberry Engineering
- Resources from PayloadsAllTheThings
- Encyclopedia on Hacking the Cloud - (No content yet for Azure)
- azure-security-lab - Securing Azure Infrastructure - Hands on Lab Guide
- AzureSecurityLabs - Hands-on Security Labs focused on Azure IaaS Security
- Building Free Active Directory Lab in Azure
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md
- https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security/fundamentals/pen-testing.md
- https://github.com/swiftsolves-msft/AzurePenTestScope

What is AWS
- https://docs.aws.amazon.com/
- https://github.com/awsdocs

Extras Resources
- https://github.com/enaqx/awesome-pentest
- https://www.sans.org/cyber-security-courses/cloud-penetration-testing/
- https://www.udemy.com/course/cloud-hacking/
- https://aws.amazon.com/pt/security/penetration-testing/
- https://cloudacademy.com/course/aws-security-fundamentals/introduction-74/
- https://cobalt.io/blog/what-you-need-to-know-about-aws-pentesting
- https://gracefulsecurity.com/an-introduction-to-penetration-testing-aws-same-same-but-different/
- https://www.virtuesecurity.com/aws-penetration-testing-part-2-s3-iam-ec2/
- https://securityboulevard.com/2021/03/aws-penetration-testing-essential-guidance-for-2021/
- https://www.darkskope.com/aws-penetration-testing
- https://bootcamps.pentesteracademy.com/certifications
- https://docs.microsoft.com/pt-br/azure/security/fundamentals/pen-testing
- https://www.youtube.com/watch?v=IOhvlooWzOg
- https://gbhackers.com/cloud-computing-penetration-testing-checklist-important-considerations/
- https://www.linkedin.com/pulse/cloud-computing-penetration-testing-checklist-priya-james-ceh-1/
- https://www.happiestminds.com/blogs/tag/penetration-testing-checklist/
- https://blog.rsisecurity.com/how-to-conduct-cloud-penetration-testing/
- https://www.nettitude.com/uk/penetration-testing/cloud-service-testing/
- https://techbeacon.com/enterprise-it/pen-testing-cloud-based-apps-step-step-guide
- https://book.hacktricks.xyz/cloud-security/cloud-security-review
- https://medium.com/@jonathanchelmus/cloud-pentesting-for-noobs-da867d9c5ecb
- https://pt.slideshare.net/TeriRadichel/are-you-ready-for-a-cloud-pentest
- https://www.blackhillsinfosec.com/tag/pentest/
- https://www.youtube.com/watch?v=aqumgrSBDM4
- My ebook: https://drive.google.com/file/d/14rthHtAgbd--pWEmzmj4i5j59Rl6dLC1/view?usp=sharing
- https://hackerassociate.com/training-and-certification/ocpt-offensive-cloud-penetration-testing/
- https://ine.com/pages/cloudpentesting
- https://hausec.com/2020/01/31/attacking-azure-azure-ad-and-introducing-powerzure/
- https://gracefulsecurity.com/an-introduction-to-pentesting-azure/
- https://rhinosecuritylabs.com/cloud-security/common-azure-security-vulnerabilities/

My Social Networks
- https://www.linkedin.com/in/joas-antonio-dos-santos
- https://twitter.com/C0d3Cr4zy

What is Azure
- https://docs.microsoft.com/pt-br/azure/?product=featured
- https://github.com/MicrosoftDocs/azure-docs

PenTest Policy
- https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing
- https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement?rtc=1
- https://aws.amazon.com/pt/security/penetration-testing/
- https://msrc.microsoft.com/en-us/engage/pentest

AWS Security
- Defensive: Hardening, Security Assessment and Inventory
  - https://github.com/nccgroup/ScoutSuite
  - https://github.com/toniblyx/prowler
  - https://github.com/cloudsploit/scans
  - https://github.com/duo-labs/cloudmapper
  - https://github.com/duo-labs/cloudtracker
  - https://github.com/awslabs/aws-security-benchmark
  - https://github.com/arkadiyt/aws_public_ips
  - https://github.com/nccgroup/PMapper
  - https://github.com/nccgroup/aws-inventory
  - https://github.com/disruptops/resource-counter
  - https://github.com/Teevity/ice
  - https://github.com/cyberark/SkyArk
  - https://github.com/willbengtson/trailblazer-aws
  - https://github.com/lateralblast/lunar
  - https://github.com/tensult/cloud-reports
  - https://github.com/tmobile/pacbot
  - https://github.com/SecurityFTW/cs-suite
  - https://github.com/te-papa/aws-key-disabler
  - https://github.com/turnerlabs/antiope
  - https://github.com/lyft/cartography
  - https://github.com/mlabouardy/komiser
  - https://github.com/darkarnium/perimeterator
  - https://github.com/DenizParlak/Zeus
  - https://github.com/darkbitio/aws-recon
  - https://github.com/mhlabs/iam-policies-cli
  - https://github.com/toniblyx/my-arsenal-of-aws-security-tools
  - https://github.com/jassics/awesome-aws-security
- https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-cis.html

PenTest in AWS
- Offensive Security
  - https://github.com/carnal0wnage/weirdAAL
  - https://github.com/RhinoSecurityLabs/pacu
  - https://github.com/disruptops/cred_scanner
  - https://github.com/dagrz/aws_pwn
  - https://github.com/MindPointGroup/cloudfrunt
  - https://github.com/prevade/cloudjack
  - https://github.com/andresriancho/nimbostratus
  - https://github.com/zricethezav/gitleaks
  - https://github.com/dxa4481/truffleHog
  - https://github.com/securing/DumpsterDiver
  - https://github.com/gruntwork-io/cloud-nuke
  - https://github.com/ThreatResponse/mad-king
  - https://github.com/mozilla/MozDef
  - https://github.com/puresec/lambda-proxy
  - https://github.com/Static-Flow/CloudCopy
  - https://github.com/andresriancho/enumerate-iam
  - https://github.com/Voulnet/barq
  - https://github.com/RhinoSecurityLabs/ccat
  - https://github.com/bishopfox/dufflebag
  - https://github.com/splunk/attack_range
  - https://github.com/elitest/Redboto
  - https://github.com/Skyscanner/whispers
  - https://github.com/0xsha/cloudbrute
  - https://github.com/Parasimpaticki/sandcastle
  - https://github.com/smiegles/mass3
  - https://github.com/koenrh/s3enum
  - https://github.com/tomdev/teh_s3_bucketeers
  - https://github.com/eth0izzle/bucket-stream
  - https://github.com/gwen001/s3-buckets-finder
  - https://github.com/aaparmeggiani/s3find
  - https://github.com/random-robbie/slurp
  - https://github.com/clario-tech/s3-inspector
  - https://github.com/pbnj/s3-fuzzer
  - https://github.com/jordanpotti/AWSBucketDump
  - https://github.com/bear/s3scan
  - https://github.com/sa7mon/S3Scanner
  - https://github.com/magisterquis/s3finder
  - https://github.com/abhn/S3Scan
  - https://github.com/whitfin/s3-meta
  - https://github.com/whitfin/s3-meta
  - https://github.com/vr00n/Amazon-Web-Shenanigans
  - https://github.com/FishermansEnemy/bucket_finder
  - https://github.com/brianwarehime/inSp3ctor
  - https://github.com/Atticuss/bucketcat
  - https://github.com/nahamsec/lazys3
  - https://github.com/Ucnt/aws-s3-data-finder
  - https://github.com/securing/BucketScanner
  - https://github.com/VirtueSecurity/aws-extender-cli
  - https://github.com/cr0hn/festin
  - https://github.com/kurmiashish/S3Insights
  - https://github.com/nccgroup/s3_objects_check
  - https://github.com/toniblyx/my-arsenal-of-aws-security-tools
  - https://rhinosecuritylabs.com/aws/aws-essentials-top-5-tests-penetration-testing-aws/
  - https://rhinosecuritylabs.com/aws/pacu-open-source-aws-exploitation-framework/
  - https://github.com/eth0izzle/shhgit
  - https://www.getastra.com/blog/security-audit/aws-penetration-testing/
  - https://owasp.org/www-pdf-archive/Aws_security_joel_leino.pdf
  - https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-cloud-need-know/
  - https://github.com/PacktPublishing/Hands-On-AWS-Penetration-Testing-with-Kali-Linux
  - https://github.com/lamkeysing92/aws-pentest-inventory
  - https://github.com/dagrz/aws_pwn
  - https://github.com/appsecco/breaking-and-pwning-apps-and-servers-aws-azure-training