Awesome Cloud Security

⚔□⚔ Awesome curated list of cloud security resources including relevant penetration testing tools for Cloud Security

Contents

Standards

Compliances

- CSA STAR (https://cloudsecurityalliance.org/star/)
- ISO/IEC 27017:2015 (https://www.iso.org/standard/43757.html)
- ISO/IEC 27018:2019 (https://www.iso.org/standard/76559.html)
- MTCS SS 584 (https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/ComplianceAndCertification)

Benchmarks

- CIS Benchmark (https://www.cisecurity.org/cis-benchmarks/)

Tools

Infrastrcture

- aws_pwn (https://github.com/dagrz/aws_pwn): A collection of AWS penetration testing junk
- aws_ir (https://github.com/ThreatResponse/aws_ir): Python installable command line utility for mitigation of instance and key compromises.
- aws-vault (https://github.com/99designs/aws-vault): A vault for securely storing and accessing AWS credentials in development environments.
- awspx (https://github.com/FSecureLABS/awspx): A graph-based tool for visualizing effective access and resource relationships within AWS.
- azucar (https://github.com/nccgroup/azucar): A security auditing tool for Azure environments
- checkov (https://github.com/bridgecrewio/checkov): A static code analysis tool for infrastructure-as-code.
- CloudBrute (https://github.com/0xsha/CloudBrute): A multiple cloud enumerator.
- cloud-forensics-utils (%5Bhttps://github.com/google/cloud-forensics-utils): A python lib for DF & IR on the cloud.
- cloudlist (https://github.com/projectdiscovery/cloudlist): Listing Assets from multiple Cloud Providers.
- cloudgoat (https://github.com/RhinoSecurityLabs/cloudgoat): "Vulnerable by Design" AWS deployment tool.
- Cloudmapper (https://github.com/duo-labs/cloudmapper): Analyze your AWS environments.
- cloudsplaining (https://github.com/salesforce/cloudsplaining): An AWS IAM Security Assessment tool that identifies violations of least privilege and generates a risk-prioritized report.
- Cloudsploit Scans (https://github.com/cloudsploit/scans): Cloud security configuration checks.
- Cloud-custodian (https://github.com/cloud-custodian/cloud-custodian): Rules engine for cloud security, cost optimization, and governance.
- cs suite (https://github.com/SecurityFTW/cs-suite): Tool for auditing the security posture of AWS/GCP/Azure.
- diffy (https://github.com/Netflix-Skunkworks/diffy): Diffy is a digital forensics and incident response (DFIR) tool developed by Netflix.
- ElectricEye (https://github.com/jonrau1/ElectricEye): Continuously monitor AWS services for configurations.
- Forseti security (https://github.com/forseti-security/forseti-security): GCP inventory monitoring and policy enforcement tool.
- Hammer (https://github.com/dowjones/hammer): A multi-account cloud security tool for AWS. It identifies misconfigurations and insecure data exposures within most popular AWS resources.
- kics (https://github.com/Checkmarx/kics): Find security vulnerabilities, compliance issues, and infrastructure misconfigurations early in the development cycle of your infrastructure-as-code.
- Leonidas (https://github.com/FSecureLABS/leonidas): A framework for executing attacker actions in the cloud.
- Open policy agent (https://www.openpolicyagent.org/): Policy-based control tool.
- pacbot (https://github.com/tmobile/pacbot): Policy as Code Bot.
- pacu (https://github.com/RhinoSecurityLabs/pacu): The AWS exploitation framework.
- Prowler (https://github.com/toniblyx/prowler): Command line tool for AWS Security Best Practices Assessment, Auditing, Hardening and Forensics Readiness Tool.
- ScoutSuite (https://github.com/nccgroup/ScoutSuite): Multi-cloud security auditing tool.
- Security Monkey (https://github.com/Netflix/security_monkey): Monitors AWS, GCP, OpenStack, and GitHub orgs for assets and their changes over time.
- SkyArk (https://github.com/cyberark/SkyArk): Tool to helps to discover, assess and secure the most privileged entities in Azure and AWS.
- SkyWrapper (https://github.com/cyberark/SkyWrapper): Tool helps to discover suspicious creation forms and uses of temporary tokens in AWS.

- Smogcloud (https://github.com/BishopFox/smogcloud): Find cloud assets that no one wants exposed.
- TerraGoat (https://github.com/bridgecrewio/terragoat): Bridgecrew's "Vulnerable by Design" Terraform repository.
- Terrascan (https://github.com/accurics/terrascan): Detect compliance and security violations across Infrastructure as Code to mitigate risk before provisioning cloud native infrastructure.
- tfsec (https://github.com/liamg/tfsec): Static analysis powered security scanner for Terraform code.
- Zeus (https://github.com/DenizParlak/Zeus): AWS Auditing & Hardening Tool.

Container

- auditkube (https://github.com/opszero/auditkube): Audit for for EKS, AKS and GKE for HIPAA/PCI/SOC2 compliance and cloud security.
- ccat (https://github.com/RhinoSecurityLabs/ccat): Cloud Container Attack Tool.
- Falco (https://github.com/falcosecurity/falco): Container runtime security.
- mkit (https://github.com/darkbitio/mkit): Managed kubernetes inspection tool.
- Open policy agent (https://www.openpolicyagent.org/): Policy-based control tool.

SaaS

- Function Shield (https://github.com/puresec/FunctionShield): Protection/destection lib of aws lambda and gcp function.
- FestIN (https://github.com/cr0hn/festin): S3 bucket finder and content discover.
- GCPBucketBrute (https://github.com/RhinoSecurityLabs/GCPBucketBrute): A script to enumerate Google Storage buckets.
- Lambda Guard (https://github.com/Skyscanner/LambdaGuard): AWS Lambda auditing tool.
- Policy Sentry (https://github.com/salesforce/policy_sentry): IAM Least Privilege Policy Generator.
- S3 Inspector (https://github.com/kromtech/s3-inspector): Tool to check AWS S3 bucket permissions.
- Serverless Goat (https://github.com/OWASP/Serverless-Goat): A serverless application demonstrating common serverless security flaws

Native tools

- AWS
    - Artifact (https://aws.amazon.com/artifact/): Compliance report selfservice.
    - Certificate Manager (https://aws.amazon.com/certificate-manager/): Private CA and certificate management service.
    - CloudTrail (https://aws.amazon.com/cloudtrail/): Record and log API call on AWS.
    - Config (https://aws.amazon.com/config/): Configuration and resources relationship monitoring.
    - Detective (https://aws.amazon.com/detective/): Analyze and visualize security data and help security investigations.
    - Firewall Manager (https://aws.amazon.com/firewall-manager/): Firewall management service.
    - GuardDuty (https://aws.amazon.com/guardduty/): IDS service
    - CloudHSM (https://aws.amazon.com/cloudhsm/): HSM service.
    - Inspector (https://aws.amazon.com/inspector/): Vulnerability discover and assessment service.
    - KMS (https://aws.amazon.com/kms/): KMS service
    - Macie (https://aws.amazon.com/macie/): Fully managed data security and data privacy service for S3.
    - Network Firewall (https://aws.amazon.com/network-firewall/): Network firewall service.
    - Secret Manager (https://aws.amazon.com/secrets-manager/): Credential management service.
    - Security Hub (https://aws.amazon.com/security-hub/): Integration service for other AWS and third-party security service.
    - Shield (https://aws.amazon.com/shield/): DDoS protection service.
    - VPC Flowlog (https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html): Log of network traffic.
    - WAF (https://aws.amazon.com/waf/): Web application firewall service.
- Azure

    - Application Gateway (https://azure.microsoft.com/en-us/services/application-gateway/): L7 load balancer with optional WAF function.
    - DDoS Protection (https://azure.microsoft.com/en-us/services/ddos-protection/): DDoS protection service.
    - Dedicated HSM (https://azure.microsoft.com/en-us/services/azure-dedicated-hsm/): HSM service.
    - Key Vault (https://azure.microsoft.com/en-us/services/key-vault/): KMS service
    - Monitor (https://docs.microsoft.com/en-us/azure/azure-monitor/): API log and monitoring related service.
    - Security Center (https://azure.microsoft.com/en-us/services/security-center/): Integration service for other Azure and third-party security service.
    - Sentinel (https://azure.microsoft.com/zh-tw/services/azure-sentinel/): SIEM service.
- GCP
    - Access Transparency (https://cloud.google.com/access-transparency): Transparency log and control of GCP.
    - Apigee Sense (https://cloud.google.com/apigee/api-management/apigee-sense): API security monitoring, detection, mitigation.
    - Armor (https://cloud.google.com/armor): DDoS protection and WAF service
    - Asset Inventory (https://cloud.google.com/asset-inventory): Asset monitoring service.
    - Audit Logs (https://cloud.google.com/audit-logs): API logs.
    - Cloud HSM (https://cloud.google.com/hsm): HSM service
    - Context-aware Access (https://cloud.google.com/context-aware-access): Enable zero trust access to applications and infrastructure.
    - DLP (https://cloud.google.com/dlp): DLP service:
    - EKM (https://cloud.google.com/ekm): External key management service
    - Identity-Aware Proxy (https://cloud.google.com/iap): Identity-Aware Proxy for protect the internal service.
    - KMS (https://cloud.google.com/kms): KMS service
    - Policy Intelligence (https://cloud.google.com/policy-intelligence): Detect the policy related risk.
    - Security Command Center (https://cloud.google.com/security-command-center): Integration service for other GCP security service.
    - Security Scanner (https://cloud.google.com/security-scanner): Application security scanner for GAE, GCE, GKE.
    - Event Threat Detection (https://cloud.google.com/event-threat-detection): Threat dection service.
    - VPC Service Controls (https://cloud.google.com/vpc-service-controls): GCP service security perimeter control.

Penetration Testing

Enumeration

- o365creeper (https://github.com/LMGsec/o365creeper) - Enumerate valid email addresses
- CloudBrute (https://github.com/0xsha/CloudBrute) - Tool to find a cloud infrastructure of a company on top Cloud providers
- cloud_enum (https://github.com/initstring/cloud_enum) - Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud
- Azucar (https://github.com/nccgroup/azucar) - Security auditing tool for Azure environments
- CrowdStrike Reporting Tool for Azure (CRT) (https://github.com/CrowdStrike/CRT) - Query Azure AD/O365 tenants for hard to find permissions and configuration settings
- ScoutSuite (https://github.com/nccgroup/ScoutSuite) - Multi-cloud security auditing tool. Security posture assessment of different cloud environments.
- BlobHunter (https://github.com/cyberark/blobhunter) - A tool for scanning Azure blob storage accounts for publicly opened blobs
- Grayhat Warfare (https://buckets.grayhatwarfare.com/) - Open Azure blobs and AWS bucket search

Information Gathering

- o365recon (https://github.com/nyxgeek/o365recon) - Information gathering with valid credentials to Azure

- Get-MsolRolesAndMembers.ps1 (https://gist.github.com/ciphertxt/2036e614edf4bf920796059017fbbc3d) - Retrieve list of roles and associated role members
- ROADtools (https://github.com/dirkjanm/ROADtools) - Framework to interact with Azure AD
- PowerZure (https://github.com/hausec/PowerZure) - PowerShell framework to assess Azure security
- Azurite (https://github.com/FSecureLABS/Azurite) - Enumeration and reconnaissance activities in the Microsoft Azure Cloud
- Sparrow.ps1 (https://github.com/cisagov/Sparrow) - Helps to detect possible compromised accounts and applications in the Azure/M365 environment
- Hawk (https://github.com/T0pCyber/hawk) - Powershell based tool for gathering information related to O365 intrusions and potential breaches

Lateral Movement

- Stormspotter (https://github.com/Azure/Stormspotter) - Azure Red Team tool for graphing Azure and Azure Active Directory objects
- AzureADLateralMovement (https://github.com/talmaor/AzureADLateralMovement) - Lateral Movement graph for Azure Active Directory
- SkyArk (https://github.com/cyberark/SkyArk) - Discover, assess and secure the most privileged entities in Azure and AWS

Exploitation

- MicroBurst (https://github.com/NetSPI/MicroBurst) - A collection of scripts for assessing Microsoft Azure security
- azuread_decrypt_msol_v2.ps1 (https://gist.github.com/xpn/f12b145dba16c2eebdd1c6829267b90c) - Decrypt Azure AD MSOL service account

Credential Attacks

- MSOLSpray (https://github.com/dafthack/MSOLSpray) - A password spraying tool for Microsoft Online accounts (Azure/O365)
- MFASweep (https://github.com/dafthack/MFASweep) - A tool for checking if MFA is enabled on multiple Microsoft Services Resources
- adconnectdump (https://github.com/fox-it/adconnectdump) - Dump Azure AD Connect credentials for Azure AD and Active Directory

Reading Materials

AWS

- Overiew of AWS Security (https://aws.amazon.com/security/)
- AWS-IAM-Privilege-Escalation by RhinoSecurityLabs (https://github.com/RhinoSecurityLabs/AWS-IAM-Privilege-Escalation): A centralized source of all AWS IAM privilege escalation methods.
- MITRE ATT&CK Matrices of AWS (https://attack.mitre.org/matrices/enterprise/cloud/aws/)
- AWS security workshops (https://github.com/aws-samples/aws-security-workshops)
- Bucket search by grayhatwarfare (https://buckets.grayhatwarfare.com/)

Azure

- Overiew of Azure Security (https://azure.microsoft.com/en-us/overview/security/)
- Azure security fundamentals (https://docs.microsoft.com/en-us/azure/security/fundamentals/)
- MicroBurst by NetSPI (https://github.com/NetSPI/MicroBurst): A collection of scripts for assessing Microsoft Azure security

- MITRE ATT&CK Matrices of Azure (https://attack.mitre.org/matrices/enterprise/cloud/azure/)
- Abusing Azure AD SSO with the Primary Refresh Token (https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/)
- Abusing dynamic groups in Azure AD for Privilege Escalation (https://www.mnemonic.no/blog/abusing-dynamic-groups-in-azure/)
- Attacking Azure, Azure AD, and Introducing PowerZure (https://hausec.com/2020/01/31/attacking-azure-azure-ad-and-introducing-powerzure/)
- Attacking Azure & Azure AD, Part II (https://posts.specterops.io/attacking-azure-azure-ad-part-ii-5f336f36697d)
- Azure AD Connect for Red Teamers (https://blog.xpnsec.com/azuread-connect-for-redteam/)
- Azure AD Introduction for Red Teamers (https://www.synacktiv.com/posts/pentest/azure-ad-introduction-for-red-teamers.html)
- Azure AD Pass The Certificate (https://medium.com/@mor2464/azure-ad-pass-the-certificate-d0c5de624597)
- Azure AD privilege escalation - Taking over default application permissions as Application Admin (https://dirkjanm.io/azure-ad-privilege-escalation-application-admin/)
- Defense and Detection for Attacks Within Azure (https://posts.specterops.io/detecting-attacks-within-azure-bdc40f8c0766)
- Hunting Azure Admins for Vertical Escalation (https://www.lares.com/blog/hunting-azure-admins-for-vertical-escalation/)
- Impersonating Office 365 Users With Mimikatz (https://www.dsinternals.com/en/impersonating-office-365-users-mimikatz/)
- Lateral Movement from Azure to On-Prem AD (https://posts.specterops.io/death-from-above-lateral-movement-from-azure-to-on-prem-ad-d18cb3959d4d)
- Malicious Azure AD Application Registrations (https://www.lares.com/blog/malicious-azure-ad-application-registrations/)
- Moving laterally between Azure AD joined machines (https://medium.com/@talthemaor/moving-laterally-between-azure-ad-joined-machines-ed1f8871da56)
- CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory (https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/)
- Privilege Escalation Vulnerability in Azure Functions (https://www.intezer.com/blog/cloud-security/royal-flush-privilege-escalation-vulnerability-in-azure-functions/)

GCP

- Overiew of GCP Security (https://cloud.google.com/security)
- GKE security scenarios demo (https://github.com/GoogleCloudPlatform/gke-security-scenarios-demo)
- MITRE ATT&CK Matrices of GCP (https://attack.mitre.org/matrices/enterprise/cloud/gcp/)

Others

- Cloud Security Research by RhinoSecurityLabs (https://github.com/RhinoSecurityLabs/Cloud-Security-Research)
- CSA cloud security guidance v4 (https://cloudsecurityalliance.org/artifacts/security-guidance-v4/)
- Appsecco provides training (https://github.com/appsecco/breaking-and-pwning-apps-and-servers-aws-azure-training)
- Mapping of On-Premises Security Controls vs. Major Cloud Providers Services (https://www.eventid.net/docs/onprem_to_cloud.asp)

Resources

Lists and Cheat Sheets

- Azure Articles from NetSPI (https://blog.netspi.com/?s=azure)
- Azure Cheat Sheet on CloudSecDocs (https://cloudsecdocs.com/azure/services/overview/)
- Resources about Azure from Cloudberry Engineering (https://cloudberry.engineering/tags/azure/)

- Resources from PayloadsAllTheThings (https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md)
- Encyclopedia on Hacking the Cloud (https://hackingthe.cloud/) - (*No content yet for Azure*)

Lab Exercises

- azure-security-lab (https://github.com/azurecitadel/azure-security-lab) - Securing Azure Infrastructure - Hands on Lab Guide
- AzureSecurityLabs (https://github.com/davisanc/AzureSecurityLabs) - Hands-on Security Labs focused on Azure IaaS Security
- Building Free Active Directory Lab in Azure (https://medium.com/@kamran.bilgrami/ethical-hacking-lessons-building-free-active-directory-lab-in-azure-6c67a7eddd7f)

Talks and Videos

- Attacking and Defending the Microsoft Cloud (Office 365 & Azure AD (https://www.youtube.com/watch?v=SG2ibjuzRJM)
  - Presentation Slides (https://i.blackhat.com/USA-19/Wednesday/us-19-Metcalf-Attacking-And-Defending-The-Microsoft-Cloud.pdf)
- TR19: I'm in your cloud, reading everyone's emails - hacking Azure AD via Active Directory (https://www.youtube.com/watch?v=JEIR5oGCwdg)
  - Presentation Slides (https://troopers.de/downloads/troopers19/TROOPERS19_AD_Im_in_your_cloud.pdf)
- Dirk Jan Mollema - Im In Your Cloud Pwning Your Azure Environment - DEF CON 27 Conference (https://www.youtube.com/watch?v=xei8lAPitX8)
  - Presentation Slides (https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Dirk-jan-Mollema-Im-in-your-cloud-pwning-your-azure-environment.pdf)
- Adventures in Azure Privilege Escalation Karl Fosaaen (https://www.youtube.com/watch?v=EYtw-XPml0w)
  - Presentation Slides (https://notpayloads.blob.core.windows.net/slides/Azure-PrivEsc-DerbyCon9.pdf)
- Introducing ROADtools - Azure AD exploration for Red Teams and Blue Teams (https://www.youtube.com/watch?v=o5QDt30Pw_o)

Books

- Pentesting Azure Applications (https://nostarch.com/azure)

Tips and Tricks

- Replace COMPANYNAME with the company name of your choice to check if they use Azure. If the **NameSpaceType** indicates *"Managed"*, then the company is using Azure AD:

```
https://login.microsoftonline.com/getuserrealm.srf?login=username@COMPANYNAME.onmicrosoft.com&xml=1
```