Cloud Security

- **Cloud Computing Models**
  - IaaS - Infrastructure as a service
  - PaaS - Platform as a service
  - SaaS - Software as a service
- **Cloud Delployment Models**
  - Public Cloud
  - On-Premises Cloud (Private)
  - Hybrid (Cloud applications connected to private datacenter)
- **Kerbernetes (k8s)**
  - https://kerbernetes.io
  - each set of containers live in a pod and a pod is a unit of scheduling
  - Components
  - Pentesting Tools
    - https://www.github. com/aquasecurity/kube-hunter
    - https://www.inguardians.com/peirates
- **AWS**
  - **AWS Cost Planning Tools**
    - AWS TCO Calaculator
      - determine what could be saved by leveraging cloud infrastructure
      - https://awstcocalculator.com
    - AWS Simple Monthly Calculator
      - calculate the cost of running specific AWS infrastructure
      - Deprecated
    - AWS Pricing Calculator — https://calculator.aws
    - AWS Resource Tags
  - **AWS Global Infrastructure**
    - Regions
      - Each region can have multiple Availability zones
      - Region Name
        - area-sub area-number[a-z]
        - us-east-2a
    - Availability Zones
      - Consists of one or more datacenters
      - Located within the geographic area of AWS Region
    - Edge Locations
      - used as nodes for global content delivery network (CDN)
      - utilized by Amazon CloudFront and Amazon Route 53
    - https://infrastructure.aws
  - **Supporting Tools**
    - AWS Support
    - AWS Personal Health Dashboard
    - AWS Trusted Advisor
  - **Assistance for Cloud Workloads**
    - AWS Quick Starts
    - AWS Partner Network Consulting Partners
    - AWS Professional Services
  - **Interacting with AWS**
    - Web Console
    - AWS CLI
    - AWS SDK
  - **Two Types of Login users**
    - root
    - IAM User
  - **AWS Services**
    - Computing Services
      - Amazon EC2
        - Provides secure and resizable virtual servers on AWS
        - use cases
          - web application hosting
          - batch processing
          - web services endpoint (API)
          - desktop in the cloud (VPS)
        - Root Device Types
          - Instance Store — Ephemeral storage that is physically attached to the host the virtual server is running on
          - Elastic Block Store (EBS) — Persistent storage that exists separately from the host the virtual server running on
      - AWS Elastic Beanstalk
        - platform for scaling and deploying web apps and services
        - supported application platforms
          - java
          - .net
          - python
          - nodejs
          - ruby
          - php
          - go
          - docker
        - use cases
          - deploy an application with minimal knowledge of other services
          - reduce the overall maintenance needed for the application
          - few customization are required
      - AWS Lambda — Enables compute without managing servers
    - Content and Network Delivery Services
      - Amazon Route 53
        - A domain name service (DNS)
        - Highly available
        - enables global resource routing
        - global AWS service (doesn't rely on a region)
      - Amazon VPC
        - A logically isolated section of AWS Cloud where you can launch AWS Resources in a virtual network that you define
        - supports ipv4 and ipv6
        - supports public and private subnets
        - can utilize NAT
        - supports private connection to many AWS Services
        - enables a connection to your data center
        - can connect to other VPCs
      - AWS Direct Connect — A cloud service solution that makes it easy to establish a dedicated network connection from your data center to AWS
      - Amazon API Gateway
        - Fully manages API management servife
        - directly integrates with multiple AWS services
        - provides monitoring and metrics on API calls
        - supports VPC and on-premise private applications
      - Amazon CloudFront
        - Content delivery Network (CDN)
        - enables users to get content from server closest to them
        - supports static and dynamic content
        - utilize AWS edge locations
        - includes advanced security features
          - AWS Shield for DDoS
          - AWS WAF
      - Elastic Load Balancing
        - distributes traffic across multiple targets
        - integrates with EC2, ECS, and Lambda
        - supports one or more Availability Zones
        - three types of load balancers
      - AWS Global Accelerator
        - A networking service that sends your user's traffic though AWS's global network infrastructure, improving your internet user performance by up to 60%
        - utilizes IP addresses that route to edge locations
        - once request reaches edge locations, traffic is routed through AWS network
        - can route requests to many AWS resources
          - Network Load Balancer
          - Application Load Balancer
          - EC2 Instances
          - Elastic IP Address
        - use cases
          - non-HTTP protocol like udp or MQTT
          - Requires Static IP
          - Instant Failover
    - File Storage and Data Transfer Services
      - Amazon S3
        - Store files as objects in buckets
        - provides different storage classes for different use cases
        - stores data across multiple availability zones
        - enables URL access for files
        - offers configurable rules for data lifecycle
        - can serve as static website host
        - Non-Archival Storage Classes
          - S3 Standard
          - S3 Intelligent-Tiering
          - S3 Standard-IA
          - S3 One Zone-IA
        - S3 Transfer Acceleration — Feature that can be enables per bucket that allows for optimized uploading of data using the AWS Edge Locations as a part of Amazon CloudFront
      - Amazon S3 Glacier
        - Designed for archiving of data within S3 as separate storage classes
        - offers configurable retrieval times
        - can send files directly or through lifecycle rules in S3
        - provides two different storage classes
          - S3 Glacier
            - 90 days minimum storage duration change
            - can be retrieved in either minutes or hours
            - you pay for a retrieval fee per GB retrieved
            - over 5 times less expensive than S3 Standard storage class
          - S3 Glacier Deep Archive
            - 180 days minimum storage duration change
            - can be retrieved in hours
            - you pay a retrieval fee per GB retrieved
            - over 23 times less expensive than S3 standard storage class
      - Amazon Elastic Block Store (EBS)
        - Block storage designed to be connected to a single EC2 instance that can scale to support petabytes of data and supports multiple volume types based on need
        - enables redundancy within an Availability Zone
        - allows users to take snapshots of its data
        - offers encryption of its volumes
        - provides multiple volume types
          - general purpose SSD
          - provisioned IOPS SSD
          - throughput optimized HDD
          - cold HDD
      - Amazon Elastic File System (EFS)
        - fully manages NFS file system
        - designed specifically for Linux workloads
        - supports up to petabytes scale
        - stores data across multiple AZ's
        - provides two different storage classes
          - standard
          - infrequent access
        - provides configurable lifecycle data rules
        - Amazon FSx for Windows File Server
          - fully managed native Windows File System
          - includes native Windows features
            - SMB support
            - Active Directory integration
            - Windows NTFS
            - utilizes SSD Drives for low latency
      - AWS Snowball
        - Service to physically migrate petabytes of data to AWS
        - physical device is delivered by AWS
        - you connect the Snowball to your network and upload your data
        - device is returned by a local carrier
        - AWS receives device and loads your data into S3
      - AWS Snowmobile
        - Service to physically migrate exabytes of data to AWS
        - Ruggedized shipping container is delivered to your location
        - AWS set up a connection to your network
        - you load your data on the Snowmobile
        - AWS will load data into S3 when the container is received at an AWS location
    - Database Services and Utilities
      - Amazon RDS
        - fully managed service for relational databases
        - handles provisioning, patching, backup and recovery of your database
        - supports deployment across multiple availability zones
        - launches into a VPC
        - provides both general purpose SSD and provisioned IOPS SSD drive options
        - supported platforms
          - MySQL
          - PostgressSQL
          - MariaDB
          - Oracle Database
          - SQL Server
          - Amazon Aurora
      - Amazon Aurora — is a MySQL and PostgressSQL compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open-source databases
      - Amazon DynamoDB
        - fully managed NoSQL database service
        - provides key-value and document database
        - enables extremely low latency at virtually any scale
        - supports automated scaling based on configuration
        - offers in-memory cache with DynamoDB Accelerator (DAX)
        - can handle more than 10 trillion requests per day and can support peaks of more than 20 millions requests per second
        - use cases
          - scale without excessive maintenance
          - serverless applications
          - implementations where low latency is key
          - data models without BLOB storage
      - Amazon Redshift
        - scalable data warehouse service
        - supports petabyte scale warehousing of data
        - leverages high performance disks and columnar storage
        - offers the ability to fully encrypt contents
        - provides isolation with VPC
        - enables querying of exabytes of data in Amazon S3 using Redshift Spectrum
      - Amazon Elasticache
        - fully managed in-memory data stores
        - supports both memcached and redis
        - provides low latency in response times
        - enables scaling and replicas to meet application demand
        - handles common use cases
          - database layer caching
          - session storage
      - AWS Database Migration Service
        - enables you to move data into AWS from existing databases
        - supports one time and continual migration of data
        - supports many popular commercial and open-source databases
        - only pay for compute leveraged in the migration process
    - App Integration Services
      - Amazon Simple Notification Service (SNS)
        - fully Managed pub/sub messaging service
        - enables you to create decoupled applications
        - organized according to topics
        - integrates with multiple AWS services
        - provides end user notifications across SMS, email and push notifications
      - Amazon Simple Queue Service (SQS)
        - fully Managed message queue service
        - enables you build decoupled and fault tolerant applications
        - supports up to 256 KB data payload
        - allows messages to be stored up to 14 days
        - provides two types of queues
          - standard queue
          - FIFO queue (first in first out)
      - AWS Step Functions
        - Serverless workflow management service
        - enables orchestration of workflows through a fully managed service
        - supports serverless architectures
        - can support complex workflows including error handling
        - charged per state transition along with the other AWS services leveraged
        - workflows are defined using Amazon State Language
    - Management and Governance Services
      - AWS CloudTrail
        - A service that continually log, monitor, and retain account activity related to actions across your AWS infrastructure
        - provides event history of your AWS account activity, including actions taken through the AWS management console, AWS SDKs, CLI and other AWS Services
        - inserts audit trail in an S3 bucket or into CloudWatch logs
        - logs events in the regions in which they occur
        - meets many compliance requirements for infrastructure auditing
        - as a best practice, it should be enabled on every AWS account
        - can be consolidated into an organizational trail using AWS Organizations
        - use cases
          - compliance requirement
          - forensic analysis
          - operational anlaysis
          - troubleshooting
      - AWS CloudFormation
        - managed service for provisioning infrastructure based on templates
        - no additional charge
        - templates can be YAML or JSON
        - enables infrastructure as code
        - manages dependencies between resources
        - provides drift detection to find changes in your infrastructure
      - Amazon CloudWatch
        - monitoring and management service
        - collects logs, metrics, and events from most AWS services
        - enables alarms based on metrics
        - provides visualization capabilities for metrics
        - allows for custom dashboards based on collected metrics
      - AWS Config
        - provides configuration history for infrastructure
        - works against rules that you can customize or even create custom validations
        - includes conformance packs for compliance standards including PCI-DSS
        - can work with AWS Organizations for both cross-region and cross-account setup
        - provides remediation steps for infrastructure not meeting criteria
      - AWS Systems Manager
        - provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources
        - provides multiple tools that make it easier to manage your AWS infrastructure
        - enables automation tasks for common maintenance actions
        - gives a secure way to access servers using AWS Credentials only
        - stores commonly used parameters securely for operational use (like database passwords)
      - AWS OpsWorks
        - configuration management service
        - provides managed instances of Chef and Puppet
        - configuration is defined as code for servers
        - Chef and Puppet manage the lifecycle of those configuration changes with servers
        - works in a hybrid cloud architecture for both cloud-based and on-premise servers
        - subservices
          - OpsWorks for Chef Automate
          - OpsWorks for Puppet Enterprise
          - OpsWorks for Stacks
      - AWS Organizations
        - allows organizations to manage multiple accounts under a single master account
        - provides organizations with the ability to leverage Consolidated Billing for all accounts
        - enables organizations to centralize logging and security standards across accounts
      - AWS Control Tower
        - a service to create a multi-account environment on AWS that follows the recommended best practices in operational efficiency, security and governance
        - centralize users across all AWS accounts
        - provides a way to create new AWS accounts based on templates
        - integrates Guardrails for accounts
        - includes a dashboard to gain operational insights from a single view
  - **AWS Architecture Core Concepts**
    - Acceptable Use Policy
      - sending unsolicited mass emails is prohibited
      - hosting or distributing harmful content is prohibited
      - penetration tests are allowed for a list of specific services
    - Least Privilege Access — when granting permission for a user to access AWS resources, you should grant them the minimum permissions needed to complete their tasks and no more
    - AWS Shared Responsibility Model
      - AWS is responsible for the security of the cloud
        - access & training for Amazon employees
        - global data centers and underlying network
        - hardware for global infrastructure
        - configuration management for infrastructure
        - patching cloud infrastructure and services
      - Customer is responsible for the security in the cloud
        - individual access to cloud resources and training
        - data security and encryption (at rest and in transit)
        - operating systems, network, and firewall configuration
        - all code deployed onto cloud infrastructure
        - patching guest operating systems and custom applications
    - AWS Well-architected Framework
      - a collection of best practices across five key pillars for how to best create systems that create business value on AWS
      - 5 Key Pillars
        - Operational Excellence — Running and monitoring systems for business value
        - Security — Protecting information and business assets
        - Reliability
          - Enabling infrastructure to recover from disruptions
          - Fault Tolerance — being able to support the failure of components within your architecture
          - High Availability — keeping your entire solution running in the expected manner despite issues that may occur
        - Performance Efficiency — Using resources efficiently to achieve business value
        - Cost Optimization — Achieving minimal costs for the desired value
      - https://aws.amazon. com/architecture/well-architected
    - Compliance
      - Common Standards
        - PCI-DSS — for processing credit cards
        - HIPAA — for healthcare date
        - SOC1,SOC2,SOC3 — third-part reviews for operational processes
        - FedRAMP — for US government data handling
        - ISO 27018 — for handling personally identifiable information
      - AWS Compliance Services
        - AWS Config — provides conformance packs for standards
        - AWS Artifact — provide self-service access to reports
        - Amazon GuardDuty — provides intelligent threat detection
    - Penetration Testing Policy
      - https://aws.amazon. com/security/penetration-testing
      - Permitted Services
        - AWS EC2, NAT Gateway, Elastic Load Balancers
        - AWS RDS, CloudFront, Aurora, API Gateway
        - AWS Lambda, Lambda Edge
        - AWS LightSail, Elastic Beanstalk
  - **AWS Identities and User Management**
    - A service that controls access to AWS resources
    - using the service is free of charge
    - manages both authentication and authorization
    - supports identity federation though SAML providers including Active Directory
    - IAM Identities
      - Users — account for a single individual to access AWS resources
      - Groups — allows you to manage permissions for a group of IAM users
      - Roles — enables a user or AWS service to assume permissions for a task
    - IAM Policies
      - a JSON document that defines permissions for an AWS IAM identity (principal)
      - defines both the AWS services that the identity can access and what actions can be taken on that service
      - can be either customer managed or managed by AWS
    - Best Practices
      - multi-factor authentication
      - least privilege acces
    - Amazon Cognito
      - A managed service that enables you to handle authentication and aspects of authorization for your custom web and mobile applications through AWS
      - user directory service for custom applications
      - provide UI components for many platforms
      - provides security capabilities to control account access
      - enables controlled access to AWS resources
      - can work with social and enterprise identity providers
        - google
        - amazon
        - facebook
        - microsoft active directory
        - SAML 2.0 providers
    - Permission Booundaries — these are permissions that can NOT be overridden at all, no matter how much power the account has
  - **AWS Data Architecture**
    - On-Premise Data Integration Services
      - AWS Storage Gateway
        - integrates cloud storage into your local network
        - deployed as a VM or specific hardware appliance
        - integrates with S3 and EBS
        - supports three different gateway types
          - tape gateway — enables tape backup processes to store data in the cloud on virtual tapes
          - volume gateway — provides cloud based ISCSI volumes to local applications
          - file gateway — stores files in Amazon S3 while providing cached low-latency local access
      - AWS DataSync
        - leverages the DataSync agent deployed as a VM on your network
        - integrates with S3, EFS, and FSx for Windows File Server on AWS
        - greatly improved speed of transfer due to custom protocol and optimizations
        - charged per GB of data transferred
    - Data Processing Services
      - AWS Glue
        - fully managed ETL (extract, transform and load) service on AWS
        - supports data in Amazon RDS, DynamoDB, Redshift and S3
        - supports a serverless model of execution
      - Amazon EMR (Elastic MapReduce)
        - enables big-data processing on Amazon EC2 and S3
        - supports popular open-source frameworks and tools
          - Apache Spark
          - Apache Hive
          - Apache Flink
          - Apache Hudi
          - Apache HBase
          - Presto
        - operated in a clustered environment without additional configuration
        - supports many different big-data use cases
      - AWS Data Pipeline
        - fully managed ETL (extract, transform and load) service on AWS
        - supports data in Amazon RDS, EMR, DynamoDB, Redshift and S3
        - manages data workflows through AWS services
        - can integrate on-premise data stores
    - Data Analysis Services
      - Amazon Athena
        - fully managed serverless service
        - enables querying of large-scale data stored within Amazon S3
        - queries are written using standard SQL
        - charged based on data scanned for query
      - Amazon Quicksight
        - fully managed business intelligence service
        - enables dynamic data dashboard based on data stored in AWS
        - charged on a per-user and per-session pricing model
        - multiple versions provided based on need (standard vs. enterprise)
      - Amazon CloudSearch
        - fully managed search service on AWS
        - support scaling of search infrastructure to meet demand
        - charged per hour and instance type of search infrastructure
        - enables developers to integrate search into custom applications
    - AI and Machine Learning Services
      - Amazon Rekognition
        - fully managed image and video recognition deep learning service
        - identifies objects in images
        - identifies objects and actions in videos
        - can detect specific people using facial analysis
        - supports custom labels for your business objects
      - Amazon Translate
        - fully managed service for translation of text
        - supports 54 languages
        - can perform language identification
        - works both in batch and real-time
      - Amazon Transcribe
        - fully managed speech recognition services
        - recorded speech is converted into text in custom applications
        - includes a specific sub-service for medical use
        - supports batch and real-time transcriptions
        - supports 31 languages
  - **AWS Architecting Applications**
    - on EC2
      - Horizontal Scaling Services
        - Auto Scaling Group
          - launch template defines the instance configuration for the group
          - defines the minimum, maximum and desired number of instances
          - performs health checks on each instance
          - exists within 1 or more availability zones in a single region
          - works with on-demand and spot instances
        - Elastic Load Balancer
      - Security
        - AWS Secrets Manager
          - secure way to integrate credentials, API keys, tokens and other secret content
          - integrates natively with RDS, DocumentDB and Redshift
          - can auto-rotate credentials with integrated services
          - enables fine-grained access control to secrets
        - Amazon VPC
          - Security Groups
            - serve as a firewall for your EC2 instances
            - control inbound and outbound traffic
            - works at the instance level
            - EC2 instances can belong to multiple security groups
            - VPC's have default security groups
            - must be explicitly associated with an EC2 instance
            - by default all outbound traffic is allowed
          - Network ACL's
            - works at the subnet level with an VPC
            - enables you to allow and deny traffic
            - each VPC has a default ACL that allows all inbound and outbound traffic
            - custom ACL's deny all traffic until rules are added
          - AWS VPN
            - creates an encrypted tunnel into your VPC
            - can be used to connect your data center or even individual client machines
            - supported in two services
              - site-to-site VPN
              - client VPN
        - AWS Shield
          - provides protection against DDoS attacks for apps running on AWS
          - enables on-going threat detection and mitigation
          - has two different service levels
            - standard
            - advanced
        - Amazon Macie
          - utilizes machine learning to analyze data stored in Amazon S3
          - it can detect personal information and intellectual property in S3
          - provides dashboards that show how the data is being stored and accessed
          - enables alerts if it detects anything unusual about data access
        - Amazon Inspector
          - enables scanning of Amazon EC2 instances for security vulnerabilities
          - charged by instance per assessment run
          - two types of rules packages
            - network reachability assessment
            - host assessment
    - Deploying Pre-defined Solutions on AWS
      - AWS Service Catalog
        - targeted to serve as an organizational service catalog for the cloud
        - can include single server image to multi-tier custom applications
        - enables organizations to leverage services that meet compliance
        - supports a lifecycle for services released in the catalog
      - AWS Marketplace
        - curated catalog of third-party solutions for customers to run on AWS
        - provides AMI's, CloudFormation stacks, and SaaS based solutions
        - enables different pricing options to overcome licensing in the cloud
        - charges appear on your AWS bill
    - AWS Developers Services
      - AWS CodeCommit
        - managed source control service
        - utilizes Git for repositories
        - control access with IAM policies
        - serves as an alternative to Github and Bitbucket
      - AWS CodeBuild
        - fully managed build and continuous integration service on AWS
        - don't have to worry about maintaining infrastructure
        - charged per minute for compute resources you utilize
      - AWS CodeDeploy
        - managed deployment service for deploying your custom applications
        - deploy to Amazon EC2, AWS Fargate, AWS Lambda and on-premise servers
        - provides a dashboard for deployments in the AWS Console
      - AWS CodePipeline
        - fully managed CI/CD service on AWS
        - provides the capabilities to automate building, testing and deploying
        - integrated with other developer tools as well as Github
      - AWS CodeStar
        - workflow tool that automates the use of the other developer services
        - creates a complete CI/CD toolchain for a custom application
        - provides custom dashboards and configurations in the AWS Console
        - you only charged for the other services you leverage
  - **Disaster Recovery on AWS**
    - Architectures
      - Backup and Restore
        - production data is backed up into Amazon S3
        - data can be stored in either standard or archival storage classes
        - EBS can be stored as snapshots in Amazon S3 also
        - in a disaster recovery event, a process is started to launch new environment
        - this approach has the longest recovery time
        - this approach has the least cost
      - Pilot Light
        - key infrastructure components are kept running in the cloud
        - designed tor reduce recovery time over the Backup and Restore approach
        - does incur cost of this infrastructure continually running in the cloud
        - AMI's are prepared for additional systems and can be launched quickly
      - Warm Standby
        - a scaled-down version of the full environment is running in the cloud
        - critical systems can be running on less capable instance types
        - instance types and other systems can be ramped up for disaster recovery event
        - does incur cost of the infrastructure continually running in the cloud
      - Multi Site
        - full environment is running in the cloud at all times
        - utilizes instance types needed for production not just recovery
        - provides a near seamless recovery process
        - incur the most cost over other approaches
    - Selecting Best Approach
      - Recovery Time Objective (RTO)
      - Recovery Point Objective (RPO)
  - **Penetration Testing Toolkit**
    - AWS CLI
      - Mapping EC2 Instances — `aws ec2 describe-instances | jq '.Reservations[] | .Instances[] | .PublicIpAddress'`
      - Pull out all security groups and ports — `for SG in `aws ec2 describe-instances | jq '.Reservations[] | . Instances[] | .NetworkInterfaces[] | .Groups[] | .GroupId' | awk -F\" '{ print $2 }'`; do echo $SG; aws ec2 describe-security-groups --group-id $SG | jq '. SecurityGroups[] | . IpPermissions[] | .ToPort'; echo '====';done`
      - List all S3 buckets — `aws s3 ls --profile <profile_name>`
      - Copy files from S3 bucket — `aws s3 cp s3://bucket/file /tmp/file --profile <profiel_name>`
      - Credentials and Config paths
        - /home/user/.aws/config
        - /home/user/.aws/credentials
      - Get user info — `aws iam get-user --profile <profile_name>`
      - List attached user policies — `aws iam list-attached-user-policies --profile <profile_name>`
      - Get IAM policy version — `aws iam get-policy-version --profile <profile_name> --policy-arn <policy_arn> --version-id <v1,2,3..>`
      - Get Keys for a user — `aws kms list-keys --profile <profile_name>`
      - Create keypair for an EC2 instance — `aws ec2 create-key-pair --profile <profile_name> --key-name <key_name> --query 'KeyMaterial' --output text > <key_name.pem>`
      - Spawn an EC2 instance with a specified keypair — `aws ec2 run-instance --profile <profile_name> --image-id <image_id> --iam-instance-profile <ARN_of_instance> --key-name <key_name.pem> --subnet-id <subnet_id> --security-group-ids <security_group_id> --output table`
      - Get EC2 instance IDs and their ARNs — `aws ec2 describe-instances --profile <profile_name> --query 'Reservations[].Instances[]' | jq '.[] | "\(. InstanceId) || \(.IamInstanceProfile.Arn)"'`
      - Encrypt file using KMS — `aws kms encrypt --key-id <key_id> --plaintext fileb: //<file_path> --query CiphertextBlob --output text | base64 -d | base64 -w 76 > ciphertext.txt`
      - Decrypt file using KMS — `aws kms decrypt --ciphertext-blob fileb://<(cat ciphertext.txt | base64 -d ) --output text --query Plaintext | base64 -d > decrypted.txt`
      - List Lambda Functions — `aws lambda list-functions --profile <profile_name>`
      - Invoke a Lambda function — `aws lambda invoke --function-name <funtion_name> --payload <function_inputs> outfile <file>`
      - List all EKS clusters — `aws eks list-clusters --region <region_name>`
      - Update Kubernetes Configuration — `aws eks update-kubeconfig --name <cluster_name> --region <region_name> --profile <profile_name>`
    - Kubernetes CLI
      - List Pods — `kubectl get pods`
      - Get info about a pod — `kubectl describe pod <pod_name>`
      - Get a shell on a container — `kubectl exec -it <container_name> /bin/bash`
    - Check Insecure S3 Buckets — https://buckets.grayhatwarfare.com/
    - CommonSpeak2 from Assetnote
      - A go-based application that connects to the BigQuery API service for wordlist creation
      - public datasets — https://www.reddit. com/r/bigquery/wiki/datasets
      - https://www.github. com/assetnote/commonspeak2
    - Privilege Escalation
      - Create or Apply a policy version on oneself, granting MORE privileges than originally provided
      - Create an instance Profile and attach them to existing EC2 roles
      - Create a key-pair and the run an EC2 instance with a service profile that has more privileges
      - Add user to a group which could have higher privileges
      - Attaching an existing policy to a user
    - Reading AWS IAM metadata
      - Provides the role — http://SERVER_IP/latest/meta-data/iam/security-credentials
      - Provides they key material needed — http://SERVER_IP/latest/meta-data/iam/security-credentials/<role_name>
      - Get Session Token — `TOKEN=`curl -X PUT https: //SERVER_IP/latest/api/token/ -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v https://SERVER_IP/latest/meta-data`
    - PACU tool
      - An open source AWS Exploitation Toolkit
      - https://github. com/RhinoSecurityLabs/pacu
    - Kube-Hunter — https://www.github. com/aquasecurity/kube-hunter
    - Peirates — https://www.inguardians.com/peirates
  - **Amazon ARN (Amazon Resource Names)**
    - `arn:partition:service:region: account-id:resource-id`
    - `arn:partition:service:region:account-id: resource-type:resource-id`
    - `arn:partition:service:region:account-id:resource-type/resource-id`
    - Examples — `arn:aws:iam::12345667654:user/Development/product_132/*`
- **Azure**
  - **Penetration Testing Policies**
    - https://docs.microsoft. com/en-us/azure/security/azure-security-pent-testing
    - Required Form to fill before pentesting — https://portal.msrc.microsoft. com/en-us/engage/pentest
    - Permitted Services
      - One's own virtual machine
      - Serverless functions, excluding function escapse
      - testing load
      - testing MDM and MAM policies
      - testing security monitoring
  - **Penetration Testing Toolkit**
    - Mapping Azure Resources with CLI — `az network public-ip list --o table`
- **Methodolgy**
  - **Application Mapping**
    - Find URLs, endpoints and APIs
      - Brute-force commonly used endpoint names
      - Mutate Document Type (from text/html to application/json)
      - Brute-force all HTTP methods
- **Cloud Native Applications**
  - Properties
    - container managed
    - continuously integrated/continuously tested (CI/CD)
    - orchestrated and defined
    - microservices oriented
    - measurable and observable
  - CNCF Trail Map — https://github.com/cncf/trailmap
  - Build systems
    - Jenkins
    - Travis CI
    - Atlassian Bamboo
    - Azure Pipelines
    - AWS CodeBuild
  - Artifacts of CI/CD tools
    - JENKINSFILE
    - .travis.yml
    - .circleci/config.yml
    - drone/.drone.yml
  - Tips — containers that pass builds are sometimes automatically deployed to production, if you can find your way into these containers you are now in PRODUCTION