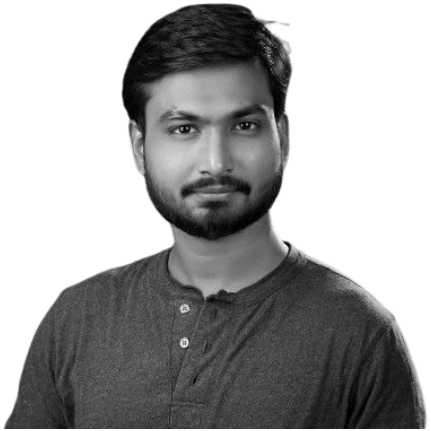
Cloud Breach Tactics

Setup VM on Cloud - tiny.cc/vulncon

Cloud Breach Tactics

Enumeration to Initial Access

About the Trainers



Chandrapal Badshah

CloudSec Consultant & Trainer

https://badshah.io

Mohit Singh

Cloud Security Engineer

https://www.linkedin.com/in/seek0/

Why did we come up with this workshop?

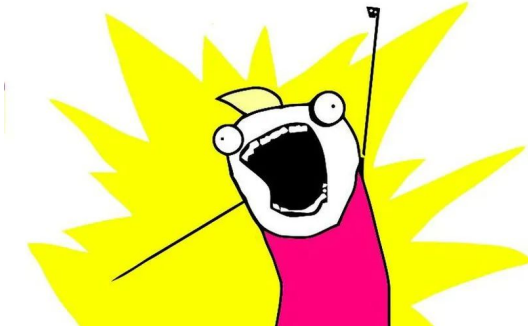
What Are We Going To Cover?

Basics of Cloud

Recon

Enumerate Cloud Footprint + Public Resources + Exposed Secrets

Pwn Target!



Timeline

10:15 - 10:55 - Intro to Cloud Security

10:55 - 11:20 - Tea Break

11:20 - 12:45 - Enumerating Cloud Footprint & Public Resource Discovery

12:45 - 2:00 - Lunch

2:00 - 4:10 - Exposed Secrets & From Discovery to Access

Before we begin

- Do **NOT** enumerate and attack websites without authorization
- We will use zomato.com for few examples. Zomato has public bug bounty program at https://hackerone.com/eternal
- Q&A at end of each session
- Setup Terraform - **tiny.cc/vulncon**

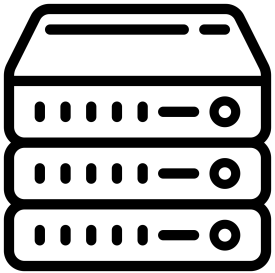
Let’s Talk “Cloud”

Cloud Providers Are Convenience Providers

Let’s assume you want to run your web app on your own server

Cloud Providers Are Convenience Providers

Let’s assume you want to run your web app on your own server



Server
Disk
Electricity

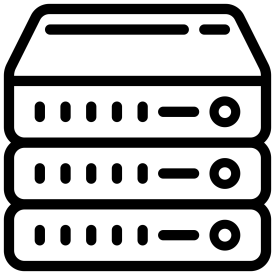
Reliable
Internet

Humans &
Automation
to Debug

Hardware
Supplier

Cloud Providers Are Convenience Providers

Cloud providers take care of these!



Server
Disk
Electricity

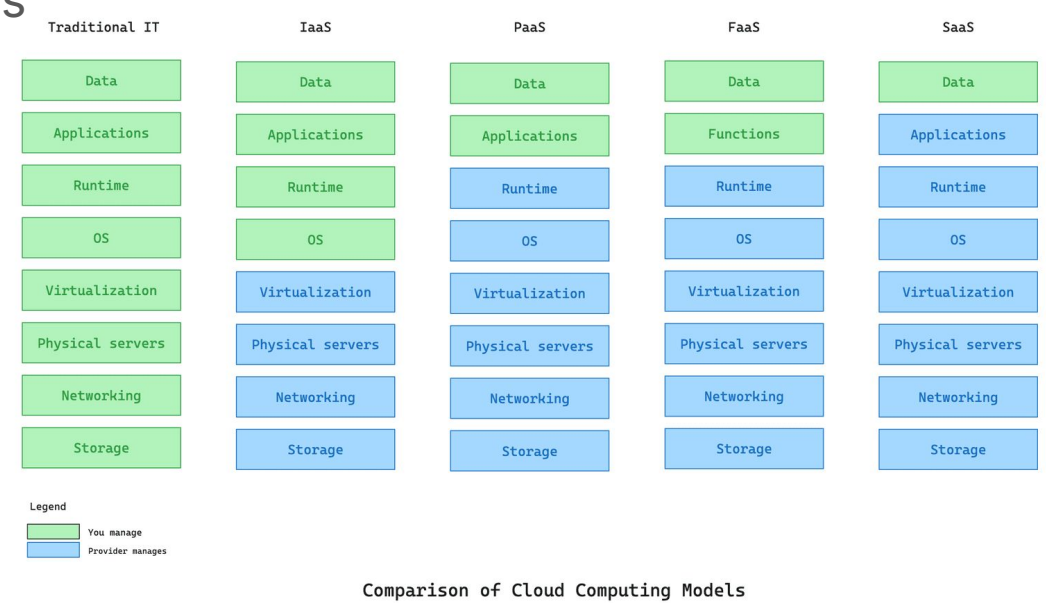
Reliable
Internet

Humans &
Automation
to Debug

Hardware
Supplier

Cloud Service Models

- Cloud provides different types of services
  - Infra as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Container as a Service (CaaS)
  - Function as a Service (FaaS)
  - Software as a Service (SaaS) - *AI services mostly fall here



Comparison of Cloud Computing Models

Source: https://strapi.io/blog/iaas-vs-paas-vs-saas-the-key-differences

Cloud Attack Surface

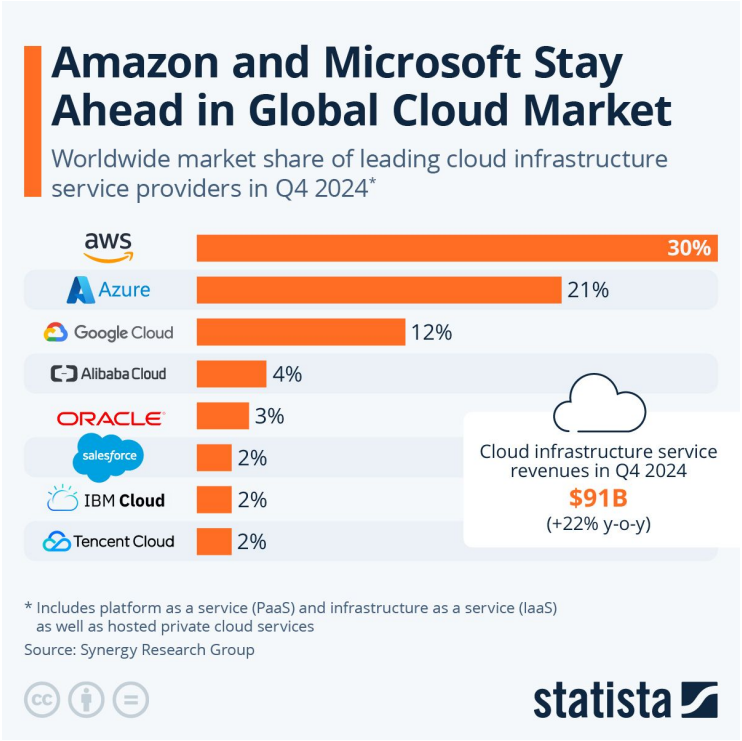
- The security boundaries of IaaS/PaaS/SaaS/etc are often blurred
- Cloud providers makes it easy for users to integrate these services

Cloud Attack Surface

- The security boundaries of IaaS/PaaS/SaaS/etc are often blurred
- Cloud providers makes it easy for users to integrate these services
- Cloud Attack Surface - all the ways an attacker can get into your environment
  - Managed databases that have default passwords/insecure configurations
  - Long lived credentials that can be accessed anywhere from internet
  - Functions having access to resources inside private network
  - SaaS services allowing user anonymous sign up
  - User created resources not following security practices
  - Susceptible to DDoS

Cloud Attack Surface In Real World

Cloud Market Share (Q4 2024)



Source: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

AWS Account Overview

- Every AWS account has 12 digit Account ID
- Root user account is the most powerful user
- **Root credential compromise = Game Over!**
- Root user must have MFA & must not have programmatic access key (but you'll still be surprised to find it)

Any Questions?

Enumerating Cloud Footprint

Look at DNS Records

- Nameserver - `dig NS example.com`
- MX Records - `dig MX example.com`
- TXT Records - `dig TXT example.com`

Example: Zomato.com

Subdomain Enumeration

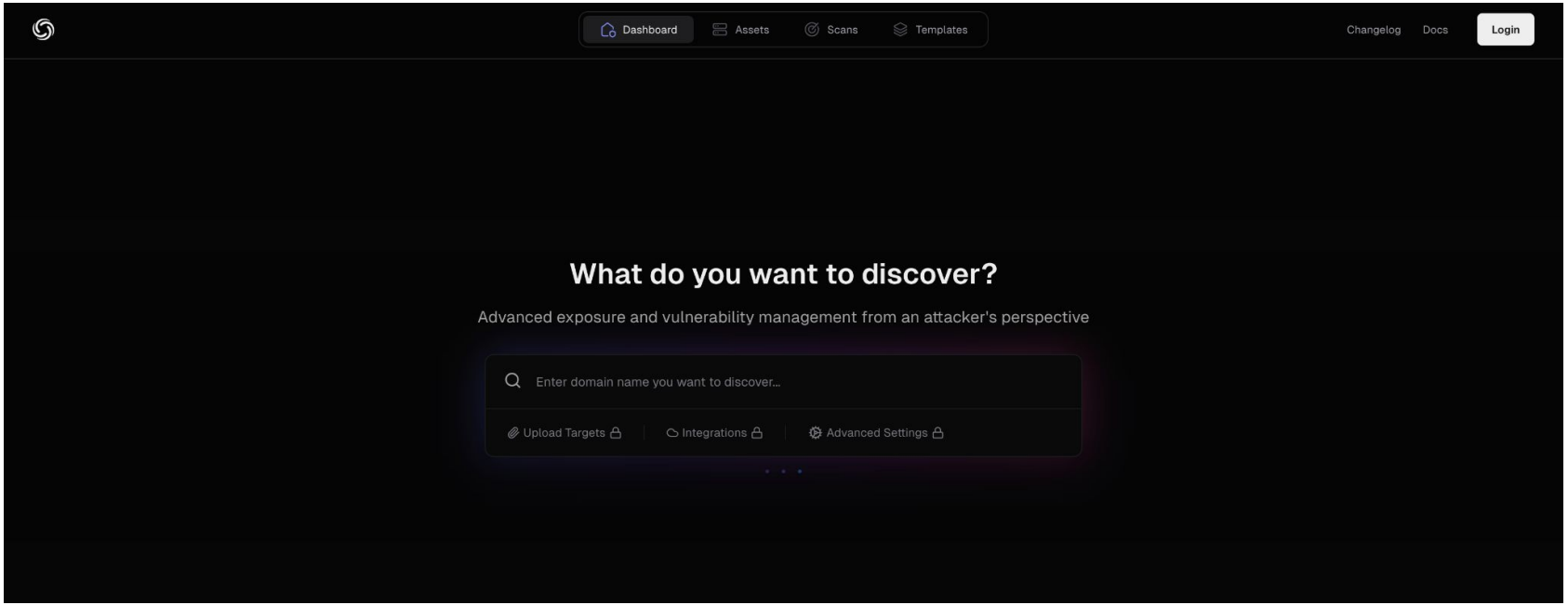
- Subdomains can give more information
- CNAME records
  - cloudfront.net, azurewebsites.net, etc
- Naming pattern
  - dev, stag, prod
  - us-east-1,
- Subfinder - `subfinder -d example.com -active`

Example: Mozilla.com

Demo 1 - Subdomain Enumeration

Do a passive enumeration of zomato.com and cloudsecurity.club

ProTip: Project Discovery



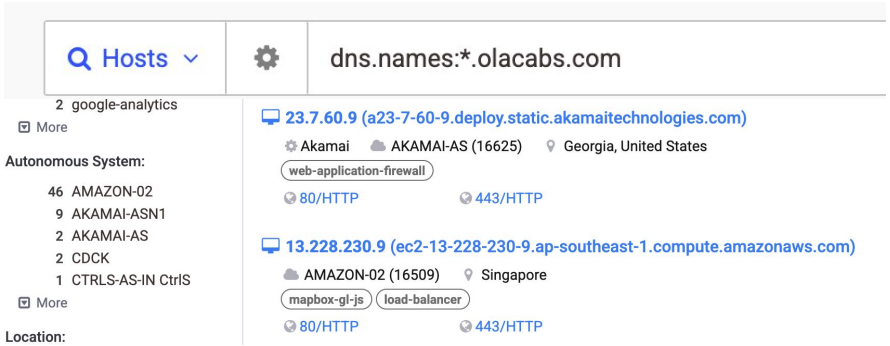
https://cloud.projectdiscovery.io

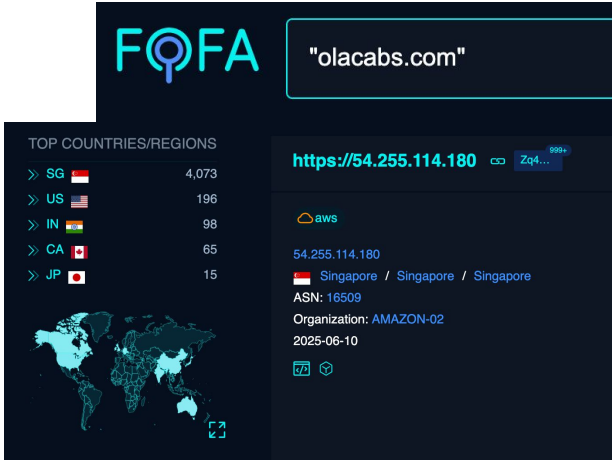
Subdomain Bruteforce

- Bruteforce to detect more subdomains
- Use naming patterns found in passive enumeration
- ShuffleDNS - `shuffledns -d hackerone.com -w wordlist.txt -r resolvers.txt -mode bruteforce`

Shodan / Censys / Fofa.info

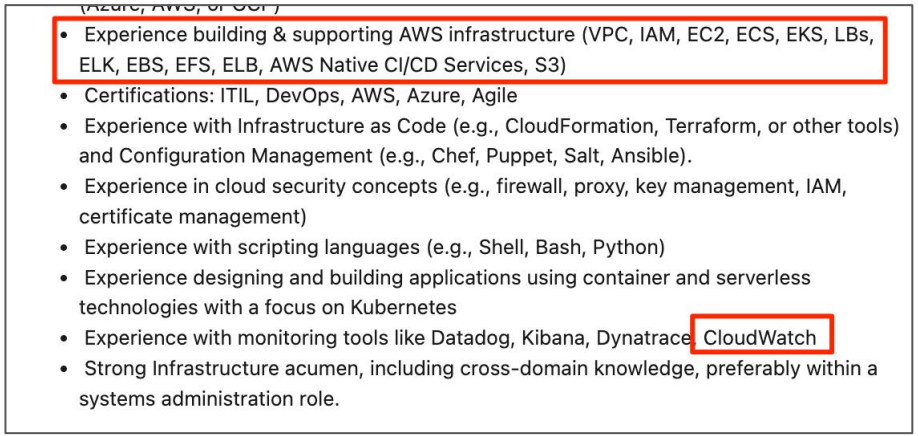
- Search engines for exposed services
- Helps identify IPs that correlate or belong to target domain
- Find regions in use and sometimes exposed databases & non-standard ports



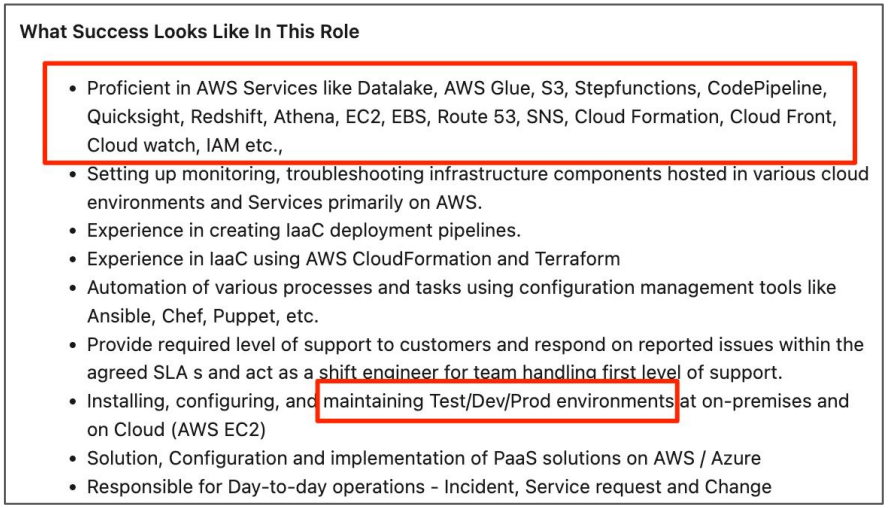


Job Descriptions & Engineering Blog Posts

Search for Cloud, Backend and Data Engineer Jobs



- Experience building & supporting AWS infrastructure (VPC, IAM, EC2, ECS, EKS, LBs, ELK, EBS, EFS, ELB, AWS Native CI/CD Services, S3)
- Certifications: ITIL, DevOps, AWS, Azure, Agile
- Experience with Infrastructure as Code (e.g., CloudFormation, Terraform, or other tools) and Configuration Management (e.g., Chef, Puppet, Salt, Ansible).
- Experience in cloud security concepts (e.g., firewall, proxy, key management, IAM, certificate management)
- Experience with scripting languages (e.g., Shell, Bash, Python)
- Experience designing and building applications using container and serverless technologies with a focus on Kubernetes
- Experience with monitoring tools like Datadog, Kibana, Dynatrace, CloudWatch
- Strong Infrastructure acumen, including cross-domain knowledge, preferably within a systems administration role.



What Success Looks Like In This Role

- Proficient in AWS Services like Datalake, AWS Glue, S3, Stepfunctions, CodePipeline, Quicksight, Redshift, Athena, EC2, EBS, Route 53, SNS, Cloud Formation, Cloud Front, Cloud watch, IAM etc.,
- Setting up monitoring, troubleshooting infrastructure components hosted in various cloud environments and Services primarily on AWS.
- Experience in creating IaaC deployment pipelines.
- Experience in IaaC using AWS CloudFormation and Terraform
- Automation of various processes and tasks using configuration management tools like Ansible, Chef, Puppet, etc.
- Provide required level of support to customers and respond on reported issues within the agreed SLA s and act as a shift engineer for team handling first level of support.
- Installing, configuring, and maintaining Test/Dev/Prod environments at on-premises and on Cloud (AWS EC2)
- Solution, Configuration and implementation of PaaS solutions on AWS / Azure
- Responsible for Day-to-day operations - Incident, Service request and Change

Any Questions?

Public Resource Discovery

Public VMs

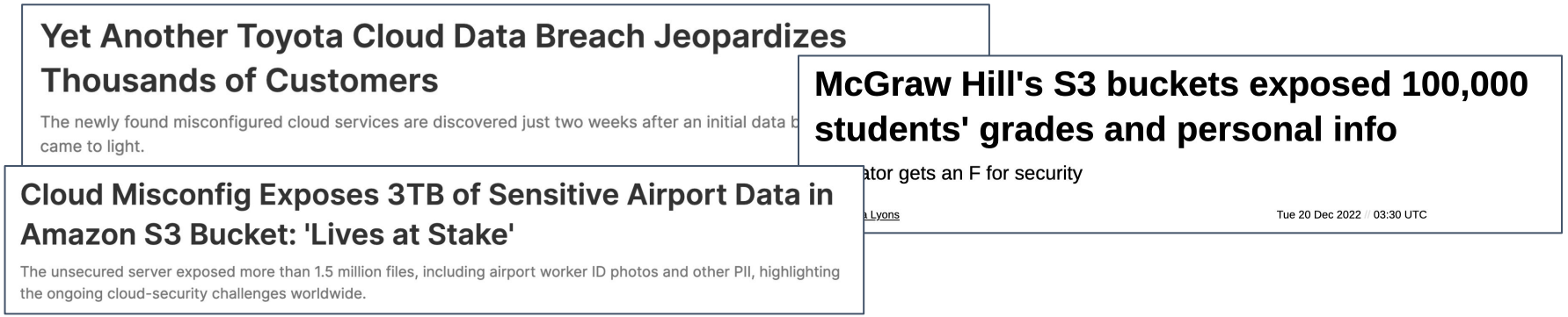
- Still the most common attack pathway.
- Developers misconfigures and/or take shortcuts to make them public
- With time they become shadows IT, easy targets of hackers.
- Common ports:
  - 80 (HTTP), 443 (HTTPS)
  - 22 (SSH), and 21 (FTP)
  - 3389 (RDP) and 53 (DNS)

Enumerating public VMs

- `subfinder -d cloudsecurity.club`
- `nmap -Pn bastion.cloudsecurity.club`
- Use hydra to bruteforce password - `hydra -l <username> -P <password-list> ssh://bastion.cloudsecurity.club`

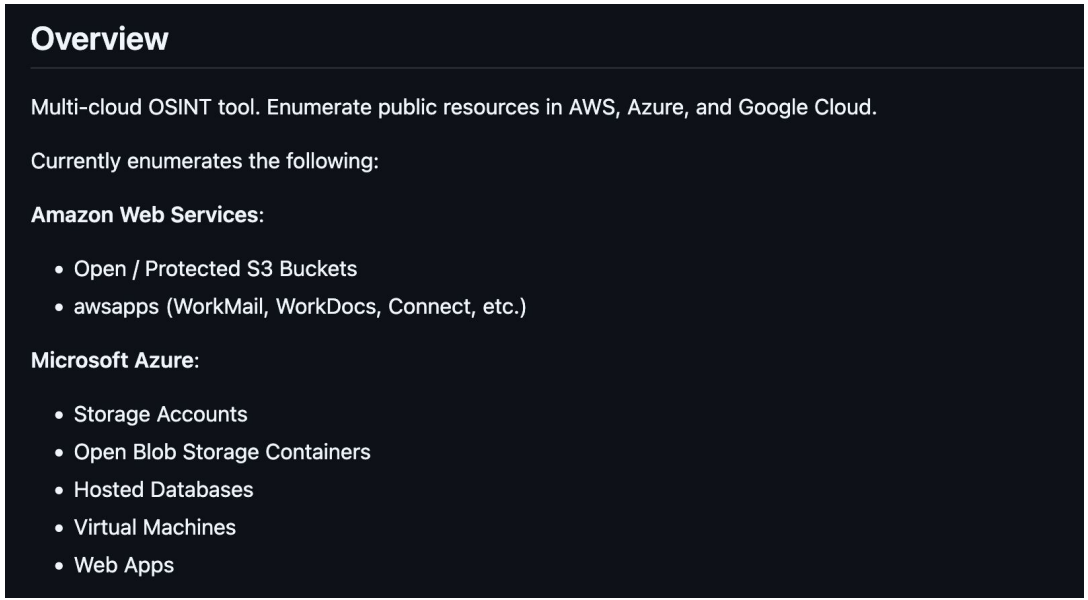
Public Buckets

- Buckets are storage repos for any type of data
- Every cloud provider supports storage buckets
  - Amazon S3
  - GCP Cloud Storage
  - Azure Blob Storage
- Public buckets are a major cause of data breaches



Enumerating Buckets

- cloud_enum - checks for existence of buckets (and other resources) across different cloud providers



Overview

Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud.

Currently enumerates the following:

Amazon Web Services:

- Open / Protected S3 Buckets
- awsapps (WorkMail, WorkDocs, Connect, etc.)

Microsoft Azure:

- Storage Accounts
- Open Blob Storage Containers
- Hosted Databases
- Virtual Machines
- Web Apps

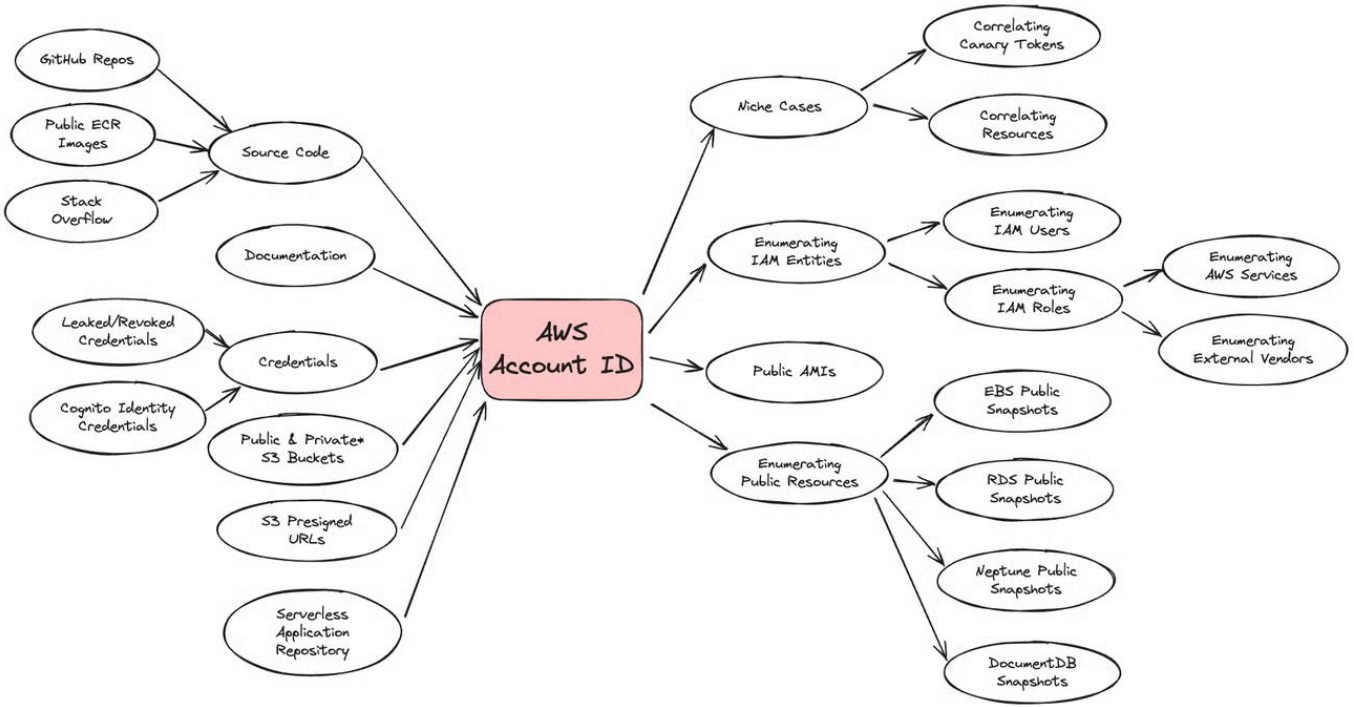
Demo 2 - Bucket Bruteforce

The admins of cloudsecurity.club have an exposed AWS S3 bucket. Find it!

AWS Account ID - The best piece of the puzzle

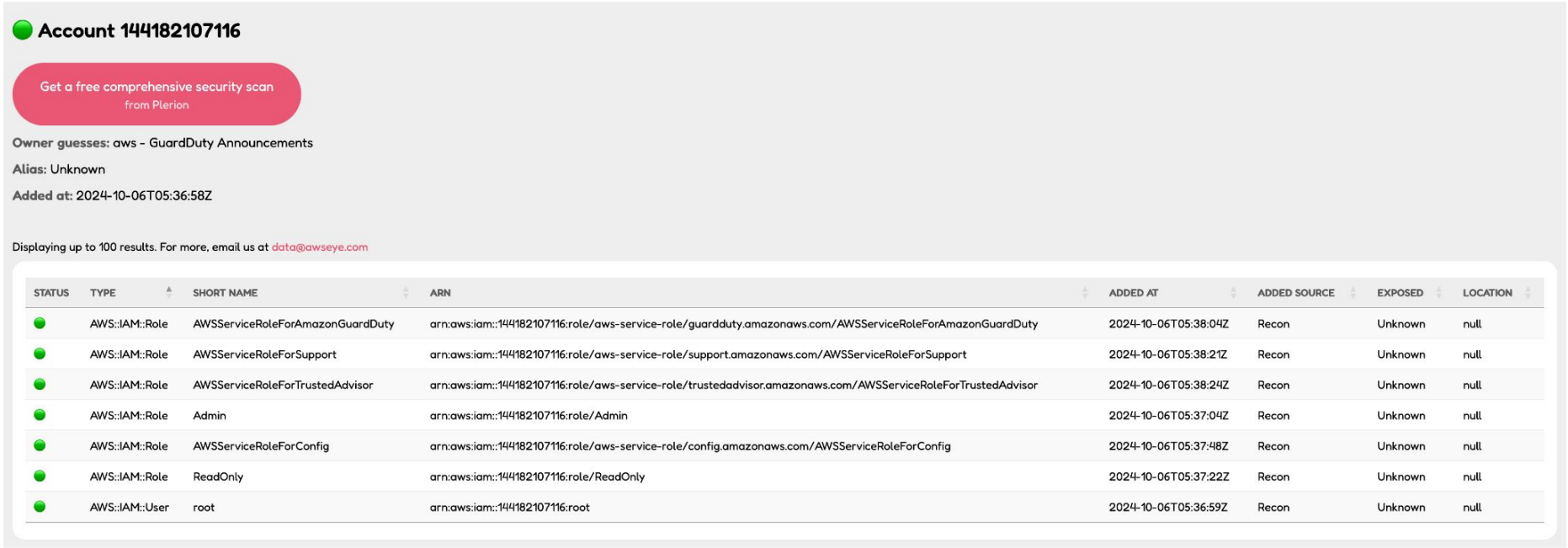
- Every AWS resource is associated with an account ID
- Looks like **123456789012**
- Ways to detect account IDs:
  - Access keys (even without the secret key)
  - Public S3 bucket object
  - GitHub repos, Documentation, etc
- You can enumerate more exposed resources using it
  - Database snapshots
  - EBS disk snapshots
  - VM Images (AMIs)

What you can do with AWS Account IDs



Source: https://cloudsecurity.club/p/well-just-aws-account-id

ProTip: awseye.com



STATUS	TYPE	SHORT NAME	ARN	ADDED AT	ADDED SOURCE	EXPOSED	LOCATION
	AWS::IAM::Role	AWSServiceRoleForAmazonGuardDuty	arn:aws:iam::1441182107116:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty	2024-10-06T05:38:04Z	Recon	Unknown	null
	AWS::IAM::Role	AWSServiceRoleForSupport	arn:aws:iam::1441182107116:role/aws-service-role/support.amazonaws.com/AWSServiceRoleForSupport	2024-10-06T05:38:21Z	Recon	Unknown	null
	AWS::IAM::Role	AWSServiceRoleForTrustedAdvisor	arn:aws:iam::1441182107116:role/aws-service-role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor	2024-10-06T05:38:24Z	Recon	Unknown	null
	AWS::IAM::Role	Admin	arn:aws:iam::1441182107116:role/Admin	2024-10-06T05:37:04Z	Recon	Unknown	null
	AWS::IAM::Role	AWSServiceRoleForConfig	arn:aws:iam::1441182107116:role/aws-service-role/config.amazonaws.com/AWSServiceRoleForConfig	2024-10-06T05:37:48Z	Recon	Unknown	null
	AWS::IAM::Role	ReadOnly	arn:aws:iam::1441182107116:role/ReadOnly	2024-10-06T05:37:22Z	Recon	Unknown	null
	AWS::IAM::User	root	arn:aws:iam::1441182107116:root	2024-10-06T05:36:59Z	Recon	Unknown	null

Demo 3 - Find exposed AMI

The devops team of cloudsecurity.club exposed an AMI publicly last week for migration and forgot to revert that change back. Can you find the account AMI.

The Account ID of cloudsecurity.club AWS account is: **593793030857**

Any Questions?

Exposed Secrets
(and where to find them)

What have we learnt so far?

- Cloud Attack Surface
  - Cloud Service Models - IaaS, PaaS, SaaS, etc
- Enumerating Cloud Footprint
  - Passive Subdomain Enumeration using Subfinder
  - Exposed service search engines - Shodan, Censys, etc
- Public Resource Discovery
  - Enumerating public buckets using cloud_enum
  - Enumerating AWS Account ID
  - Enumerating exposed resources using AWS Account ID

Coding Platforms - GitHub

- GitHub has large number of leaked secrets
- Look at interesting places
  - GitHub Actions Logs
  - GitHub Artifacts
- Note: Major cloud platforms try to disable/reduce privileges of leaked credentials

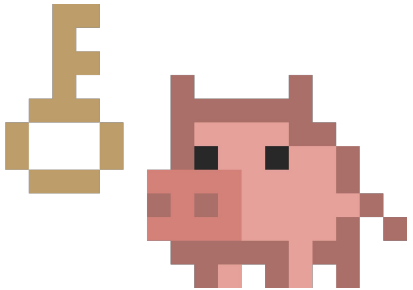
Education giant Pearson hit by cyberattack exposing customer data

An exposed GitLab token

This statement comes after sources told BleepingComputer that threat actors compromised Pearson's developer environment in January 2025 through an exposed GitLab Personal Access Token (PAT) found in a public .git/config file.

Trufflehog

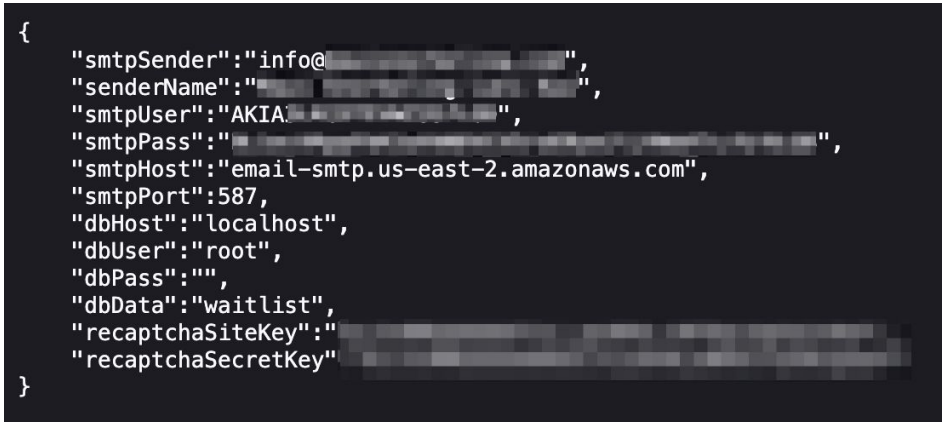
- Detects and verifies any secrets hardcoded in git repos, S3/GCS buckets, etc
- Can detect credentials of the following cloud platforms:
  - AWS
  - Azure
  - GCP
  - Others: DigitalOcean, Vultr, Heroku, etc
- Usage:
  - `trufflehog github --org=ORGNAME --results=verified`
  - `trufflehog git https://github.com/ORG/REPO.git`



Demo 4 - Trufflehog Entire Org

The admins of `CloudSecurityClub` are not securing their GitHub org repos. See if you can find any secrets!

Mobile Apps & Website JS Files

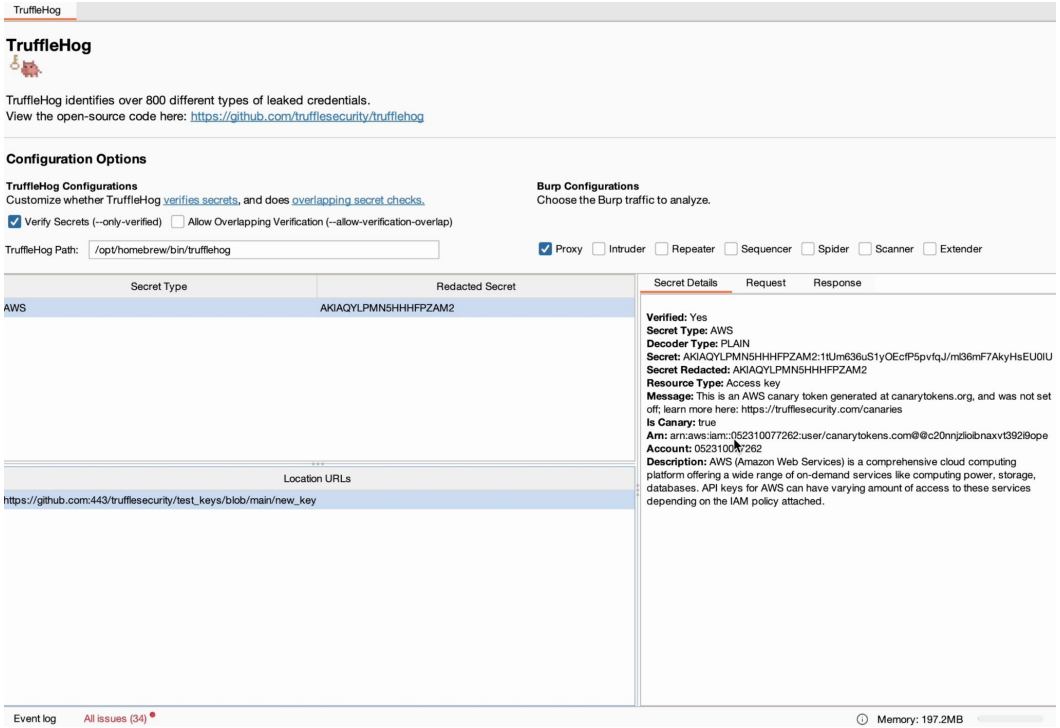


```
{
    "smtpSender":"info@[redacted]",
    "senderName":"[redacted]",
    "smtpUser":"AKIA[redacted]",
    "smtpPass":"[redacted]",
    "smtpHost":"email-smtp.us-east-2.amazonaws.com",
    "smtpPort":587,
    "dbHost":"localhost",
    "dbUser":"root",
    "dbPass":"",
    "dbData":"waitlist",
    "recaptchaSiteKey":"[redacted]
    "recaptchaSecretKey"[redacted]
}
```

```
export default {
  basename: '/',
  defaultPath: '/',
  excelConfig: {
    bucketName: '[redacted]',
    dirName: 'Excel', /* optional */
    region: 'ap-south-1',
    accessKeyId: 'AKIA[redacted]',
    secretAccessKey: '[redacted]',
  },
  videoConfig: {
    bucketName: '[redacted]',
    dirName: 'Videos', /* optional */
    region: 'ap-south-1',
    accessKeyId: 'AKIA[redacted]',
    secretAccessKey: '[redacted]',
  }
}
```

```
    <string name="default_web_client_id">[redacted].apps.googleusercontent.com</string>
    <string name="define_roundedimageview" />
    <string name="donate">捐助</string>
    <string name="firebase_database_url">https://[redacted].firebaseio.com</string>
    <string name="gcm_defaultSenderId">[redacted]</string>
    <string name="google_api_key">AIza[redacted]</string>
    <string name="google_app_id">[redacted]</string>
    <string name="google_crash_reporting_api_key">AIza[redacted]</string>
    <string name="google_storage_bucket">[redacted]ff6.appspot.com</string>
    <string name="key_account">account</string>
```

Pro Tip: Use TruffleHog Burp Suite Extension



Source: https://trufflesecurity.com/blog/introducing-trufflehog-s-burp-suite-extension-a-techical-deep-dive

Container Registries

- Container Registries are treasure troves with lots of hardcoded secrets
- Public container registries
  - DockerHub
  - GHCR.io
  - GCR.io
  - Amazon ECR

Source: https://redhuntlabs.com/blog/scanning-millions-of-publicly-exposed-docker-containers-thousands-of-secrets-leaked/

Any Questions?

From Discovery to Access

Validate AWS Access Keys

- Every IAM Access Key is associated with IAM User
- To validate if access keys are valid:
  - `aws configure set aws_access_key_id YOUR_KEY`
  - `aws configure set aws_secret_access_key YOUR_SECRET`
  - `aws sts get-caller-identity`

Permissions of AWS Access Keys

- Two Approaches
  - Gentle: List IAM policies attached
  - Harsh: Just bruteforce possible IAM action
- Gentle approach
  - `aws iam list-attached-user-policies`
  - `aws iam list-user-policies`
- Bruteforce approach
  - pacu - https://github.com/RhinoSecurityLabs/pacu

Pacu

- Open-source AWS exploitation framework developed by Rhino Security Labs
- Designed for offensive security testing and cloud penetration testing.
- Written in Python with a modular architecture.
- Key Features
  - Post-compromise tool – assumes valid AWS credentials.
  - 80+ modules to enumerate, escalate privileges, and exploit misconfigurations.
  - Supports session tracking and data persistence.

Demo: Discovery to Access using Pacu

Any Questions?

Conclusion

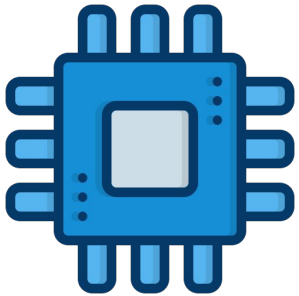
What we learnt so far?

- Cloud Attack Surface
- Enumerating Cloud Footprint
- Public Resource Discovery
- Exposed Secrets
  - Scanning using Trufflehog
  - Container Registries
- From Discovery to Access
  - Validating AWS Access keys
  - Discovery to access using Pacu

Is there a way to generalize cloud attack surface?

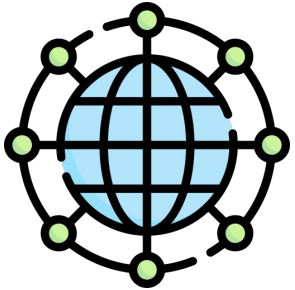
(across cloud providers)

Common Things Among Every Cloud Provider



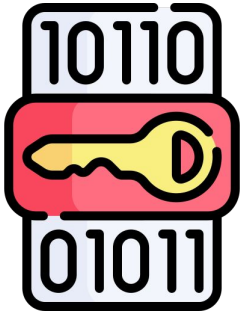
Compute

Storage



Network

Access Mgmt



Encryption

Find the flag!

The DevOps team

https://github.com/CloudSecurityClub

Resources

- Cloud Security & CTF Writeups - cloudsecurity.club
- Hacking The Cloud - hackingthe.cloud
- awesome-sec-s3 - https://github.com/mxm0z/awesome-sec-s3
- Awesome-CloudSec-Labs
- Pwned Labs
- Tl;dr sec