Pentest Tools

From bits to breaches:
the nuts and bolts of vulnerability detection in multi-cloud environments

Carina Deaconu
Ioana Stăncioiu

01.

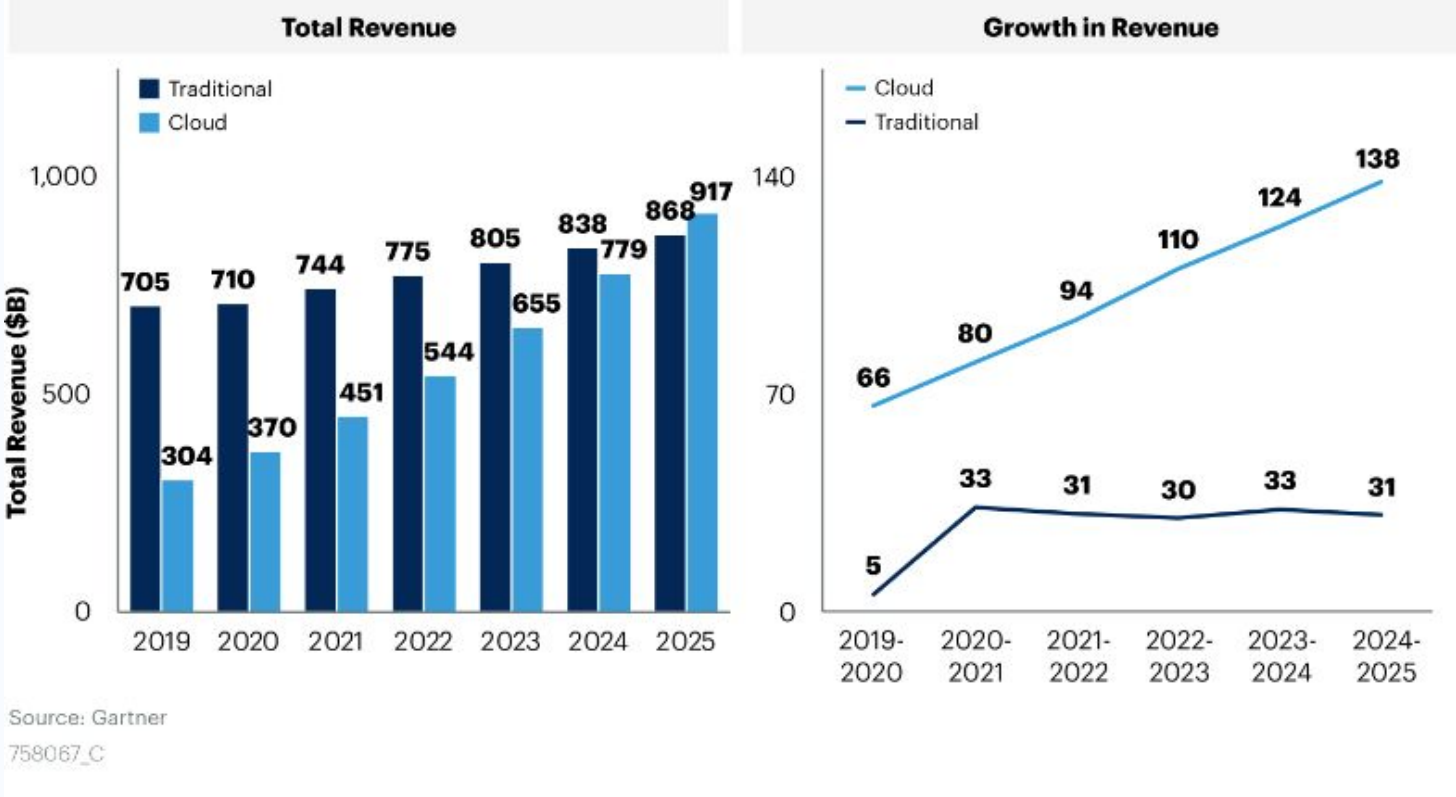
Whoarewe

- Software Engineers @Pentest-Tools.com
- Master Thesis: Vulnerabilities in Google Cloud Storage
- Bachelor Thesis: Vulnerabilities in AWS S3
- New tool on Pentest-Tools.com: Cloud Vulnerability Scanner
- Short demo at the end

02.

Why should you care about Cloud Security

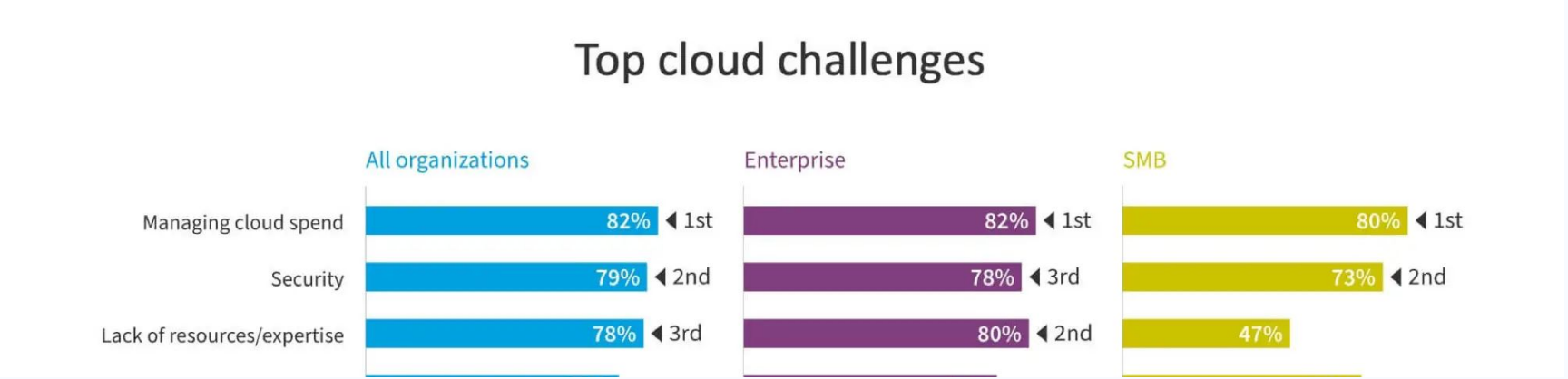
Cloud technologies are on the rise



Top cloud providers

Google Cloud

Security is a top priority



- Cloud infrastructures function by a shared responsibility model.
- Through 2025, 99% of cloud security failures will be the customer's fault.

Security incidents in recent years

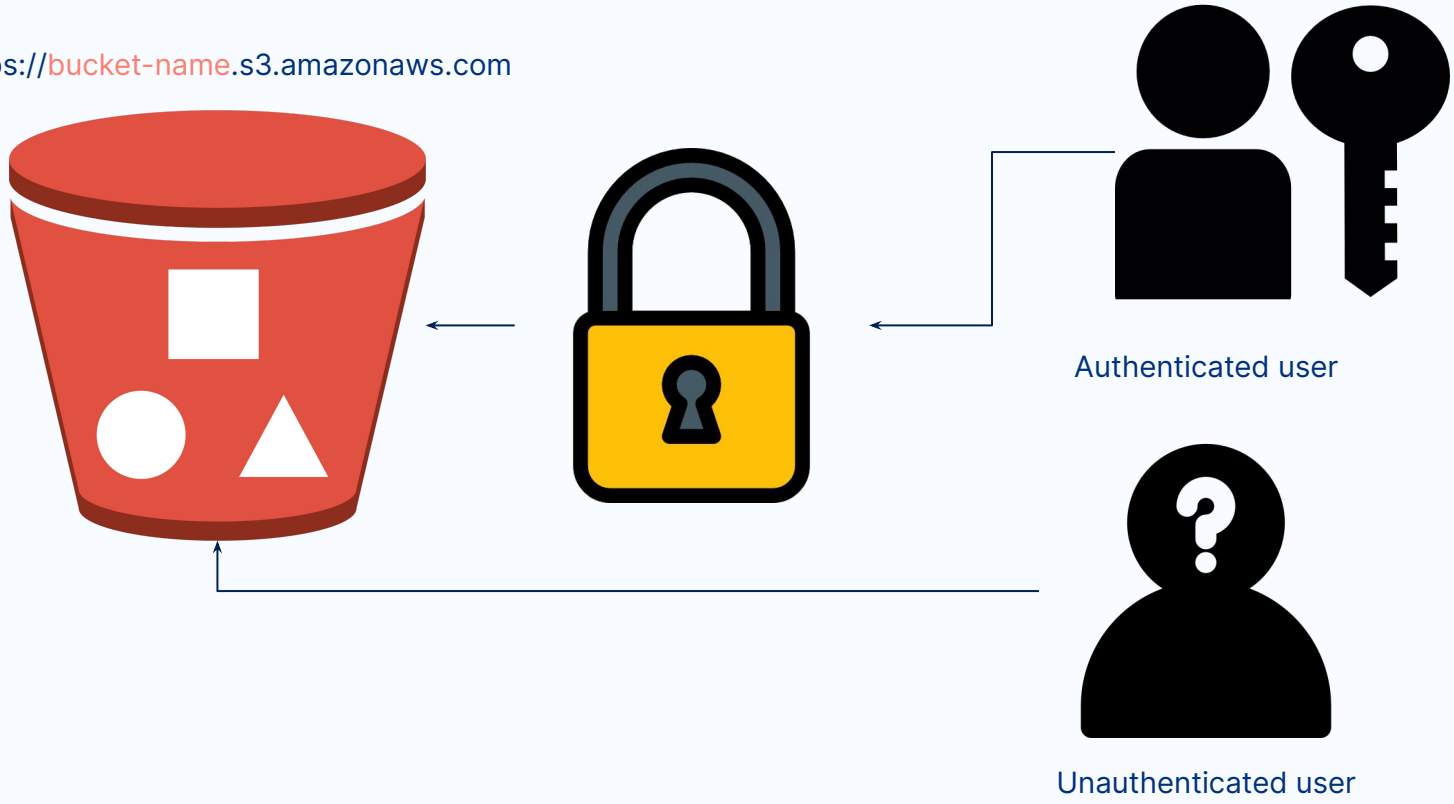
- S3 bucket misconfig of pre-signed URLs
- Cloud Misconfig Exposes 3TB of Sensitive Airport Data in Amazon S3 Bucket: 'Lives at Stake', 2022
- McGraw Hill's S3 buckets exposed 100,000 students' grades and personal info, 2022
- A famous Turkish beauty brand, Cosmolog Kozmetik, suffered a leak in its Amazon S3 bucket, 2021

03.

Hacking AWS

About AWS Simple Storage Service

https://bucket-name.s3.amazonaws.com



Relevant bucket permissions and configurations

Permissions

s3:ListBucket permission to list the bucket contents

s3:GetObject permission to read the contents of an object

s3:GetBucketACL permission to read the bucket's ACL

s3:PutObject permission to overwrite the contents of an object

s3:PutBucketACL permission to overwrite the bucket ACL and gain access to the bucket's content

Configurations

Encryption

Logging

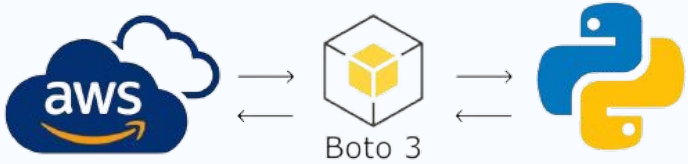
Versioning

CORS

Replication

Ownership

How we discover misconfigurations



- We use the python boto3 package to query AWS with an unauthenticated and authenticated client.
- We deliberately send POST requests with an invalid body so we don't alter the target.
- Responses differ depending on the access level:
    - 200 OK - action is permitted
    - 403 Forbidden - not authorized to perform action
    - 404 Not Found - bucket or object doesn't exist
    - 400 Bad Request - the request body is invalid, but the action is permitted

The risk of READ access

- Data breaches
- Access to documents containing sensitive information
- Helps in identifying misconfigured objects

The risk of WRITE access

- Overwriting data
- Gaining additional access to the bucket and infrastructure
- Serving malware to end users

04.

Hacking GCP

Google Cloud Storage

- A **bucket** → multiple **blobs**.
- Bucket URL: https://storage.googleapis.com/storage/v1/b/<bucket_name>

    - 404 Not Found/400 Bad Request → bucket doesn't exist
    - 403 Forbidden → buckets exists and is private (cannot be accessed without the right credentials)
    - 200 OK → bucket exists and is public to all users

Retrieving bucket permissions

- Of an unauthenticated user (= any user on the Internet)
  - Google public API
- Of an authenticated user (= a user logged in with any Google account) → service account +
  - *gcloud*
  - Python Google client

Most relevant bucket permissions

READ

- storage.buckets.get - retrieve details about a bucket;
- storage.objects.list - see bucket contents (the list of blobs);
- storage.objects.get - see the contents of a blob;
- storage.buckets.getIamPolicy - read IAM policy of the bucket;

WRITE

- storage.objects.create - add new blobs to the bucket;
- storage.objects.delete - delete blobs from the bucket;
- storage.objects.update - modify metadata of the blobs;
- storage.buckets.setIamPolicy - modify bucket ACL (⇒ priv esc!)

Privilege escalation using storage.buckets.setIamPolicy

storage.buckets.setIamPolicy

→ update IAM with role roles/storage.admin granted to allUsers

→ profit as admin

Types of access control on a bucket

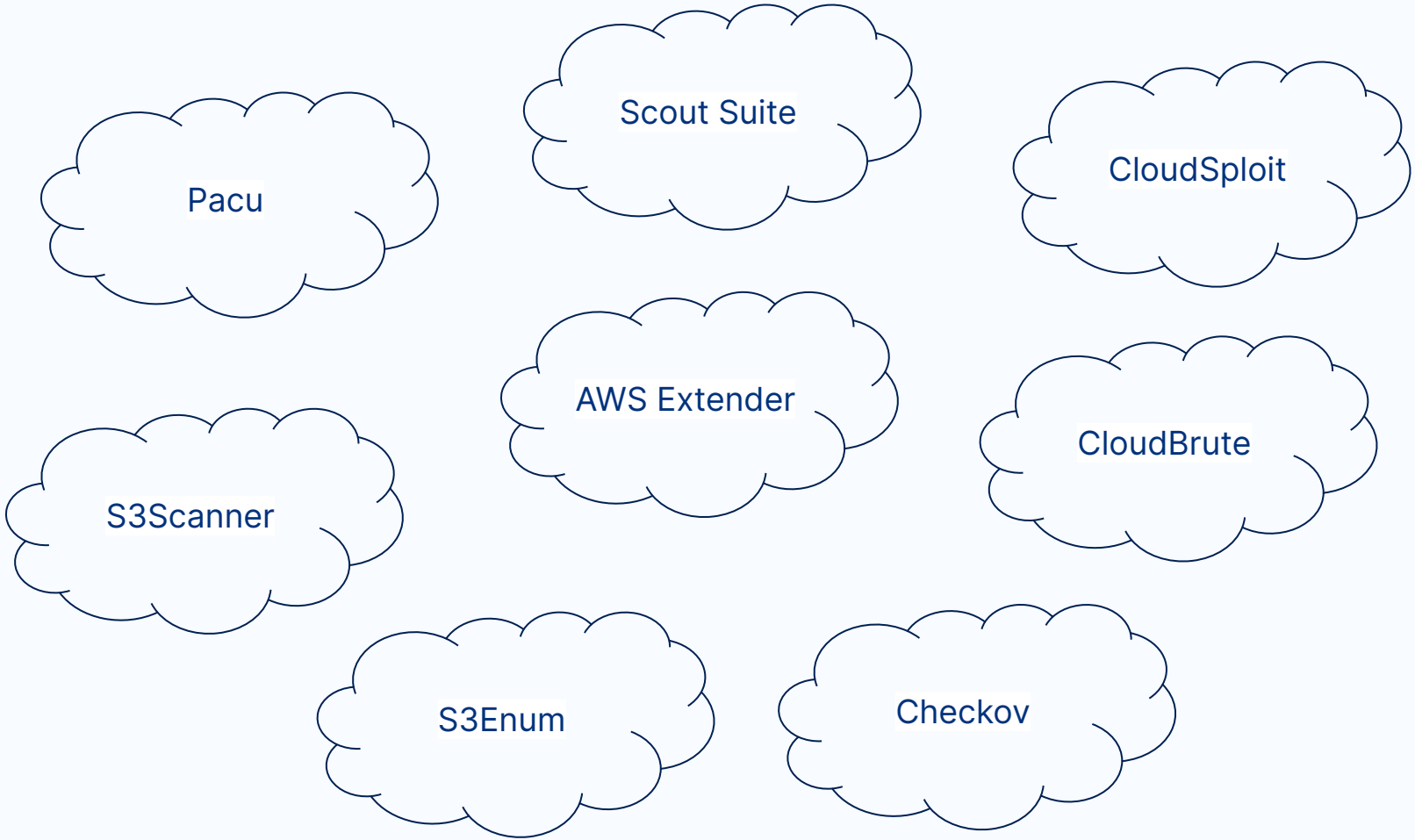
- uniform bucket-level access (default): the same set of permissions across the bucket and its objects, through bucket-level IAM
- fine-grained: different types of access to objects can be specified using object ACLs, in addition to bucket-level IAM
- default object ACL if none is specified

Relevant configurations of the bucket

- Logging
- Object versioning/retention policy
- Labels
- Object lifecycle rules
- Customer-managed encryption key
- CORS

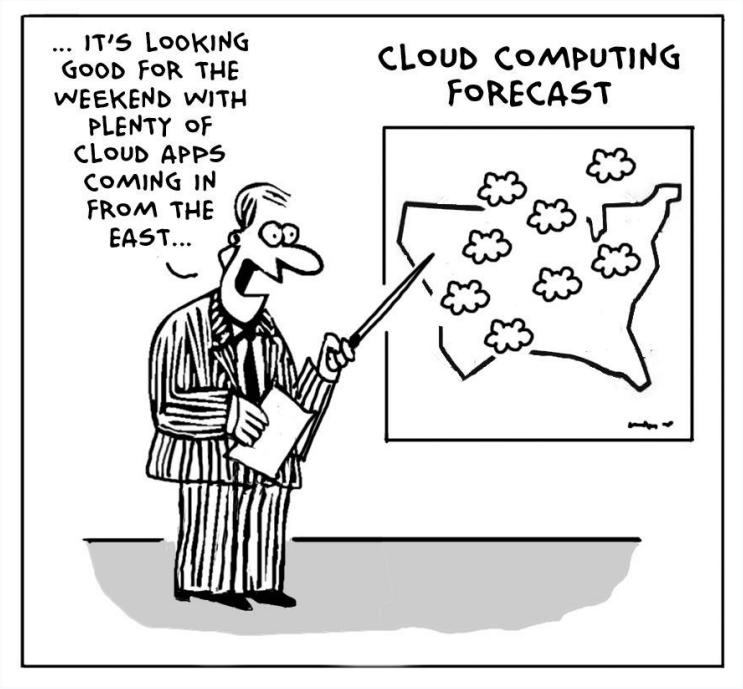
05.

Open source tools


Pacu
Scout Suite
CloudSploit
AWS Extender
S3Scanner
CloudBrute
S3Enum
Checkov

Mitigations & Good practices

- Don’t use ACLs to secure access to your bucket
- Double check bucket policies and ACLs
- Use the principle of least privilege
- Use encryption
- Enable the “Block public access” option
- Enable MFA for sensitive operations
- Monitor continuously



05.

Demo time!


I WAS HOPING FOR A SLIGHTLY MORE DETAILED EXPLANATION OF HOW CLOUD COMPUTING WORKS THAN – "IT'S MAGIC"!
IT
© D.Fletcher for CloudTweaks.com


LET US PRAY
TO THE DEMO GODS