JAY KALSI

HACKING THE CLOUD

Attacking Enterprise AWS Deployments

ABOUT ME

- Live & work in Melbourne
- Currently Leading an Offensive Security Team
- Background in PenTest, Red Team & AppSec Consulting
- Lately have been doing some IoT hacking
- Have been working in the industry since Bitcoin was < $1.00 AUD

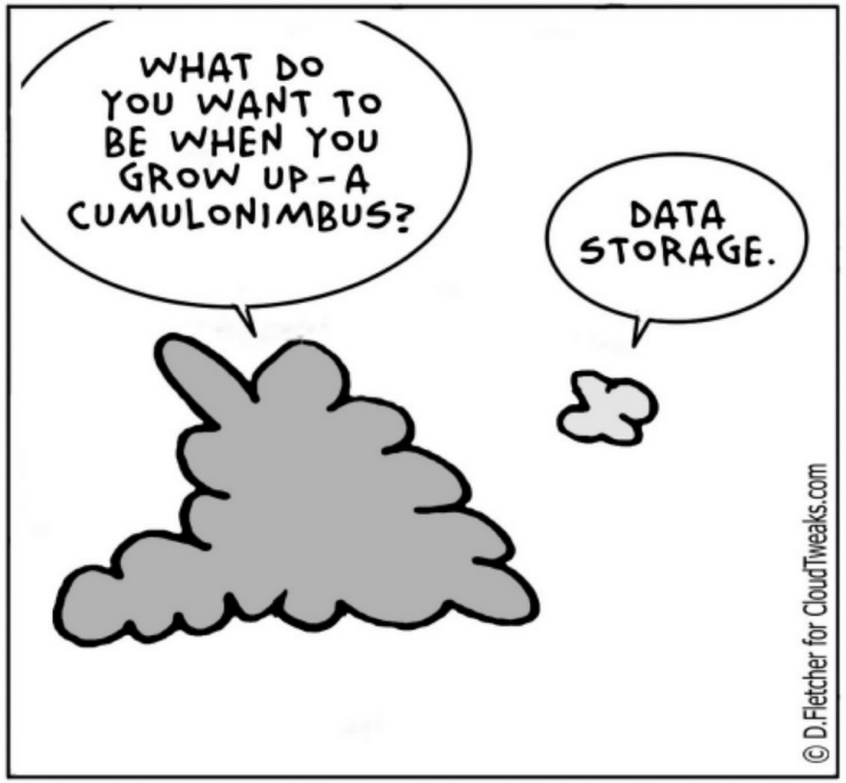
Cloud Simplified

Basically someone else's computer

“cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale”

AGENDA

- BRIEF OVERVIEW - AWS IAM
- AWS HYBRID CLOUD
- HIGH RISK SECURITY ISSUES
- LESSONS LEARNT/AVOIDING COMMON MISTAKES & DATA BREACHES
- CONCLUSION



Cloud Computing

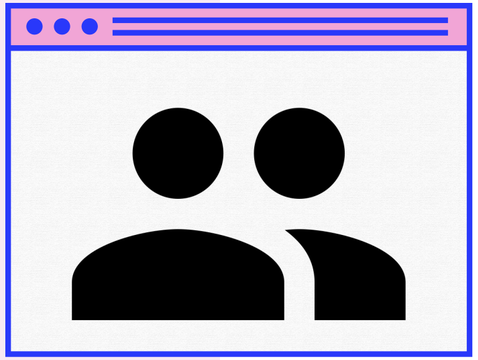
CLOUD SECURITY

OVERVIEW

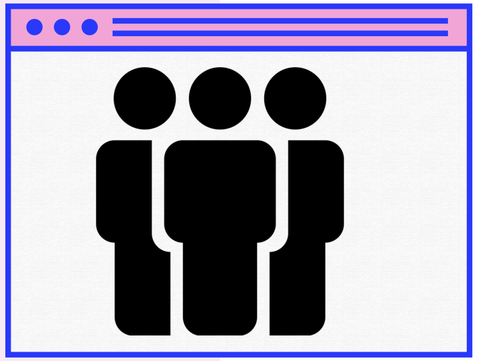
IAM - IDENTITY AND ACCESS MANAGEMENT

- CORE SERVICE BEHIND AUTHENTICATION, AUTHORISATION & ACCESS MANAGEMENT IN AWS
- EASY TO MISCONFIGURE HENCE MAIN SOURCE OF VULNERABILITIES

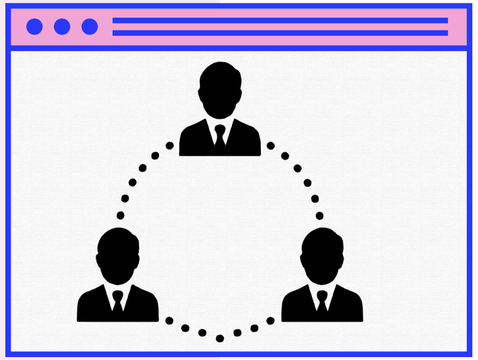
Overview of IAM



USER ACCOUNTS



GROUPS



ROLES

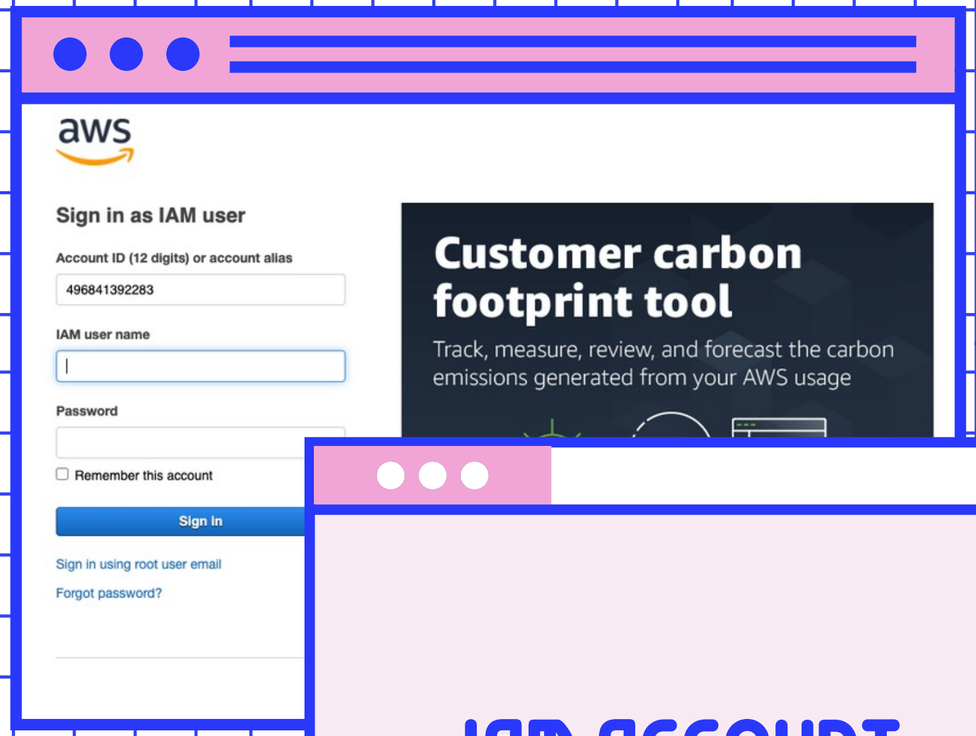
USERS

USERS CREATED IN YOUR AWS ACCOUNT

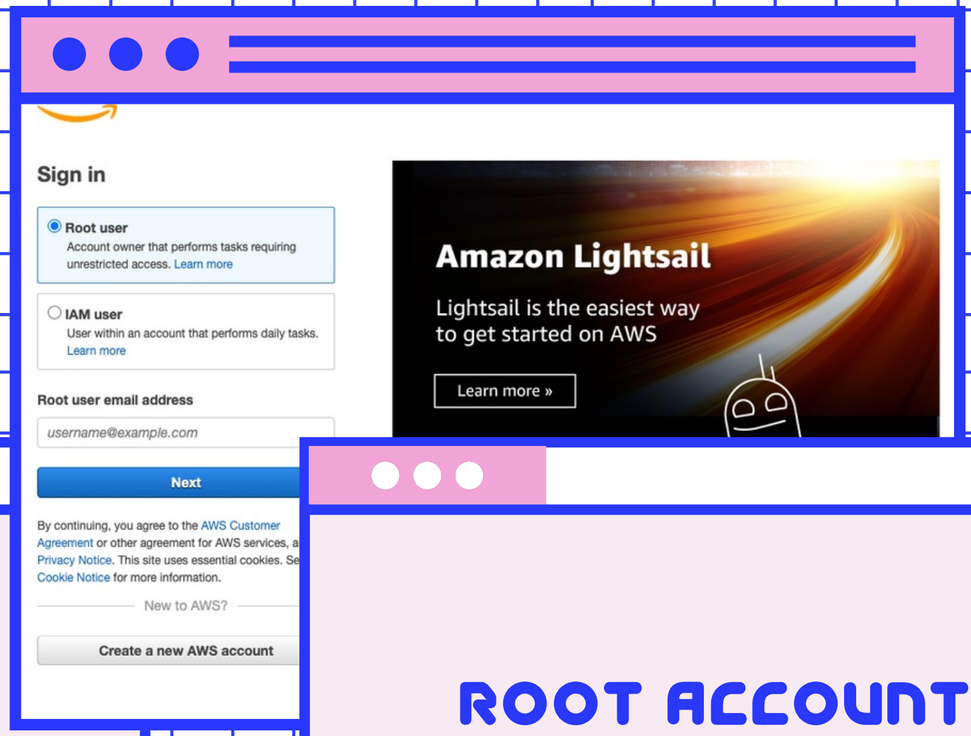
NEED A ROOT ACCOUNT TO CREATE FIRST IAM ACCOUNT

IAM ACCOUNTS CAN LOGIN USING CUSTOMER URL

https://49684546283.signin.aws.amazon.com/console



IAM ACCOUNT LOGIN



ROOT ACCOUNT LOGIN

IAM GROUPS

- COLLECTION OF IAM USERS
- A GROUP CAN CONTAIN MANY USERS
- A USER CAN BELONG TO MULTIPLE GROUPS
- GROUPS CAN'T BE NESTED

```
aws iam list-groups
```


```
{
    "Groups": [
        {
            "Path": "/",
            "GroupName": "Admin",
            "GroupId": "AGPAJ6XPJC7ZLGPURTSCM",
            "Arn": "arn:aws:iam::496841392283:group/Admin",
            "CreateDate": "2018-07-11T05:12:47Z"
        },
        {
            "Path": "/",
            "GroupName": "ReadOnly",
            "GroupId": "AGPAIDD2O2CENMNWTTNEO",
            "Arn": "arn:aws:iam::496841392283:group/ReadOnly",
            "CreateDate": "2018-07-11T05:14:35Z"
        },
        {
            "Path": "/",
            "GroupName": "SecurityAudit",
            "GroupId": "AGPAIGVVKZEOFLCOHTAOS",
            "Arn": "arn:aws:iam::496841392283:group/SecurityAudit",
            "CreateDate": "2018-07-02T23:11:33Z"
        },
        {
            "Path": "/",
            "GroupName": "Test",
            "GroupId": "AGPAIA6ZQ4WWJXGAF6J7M",
            "Arn": "arn:aws:iam::496841392283:group/Test",
            "CreateDate": "2018-07-11T05:20:50Z"
        }
    ]
}
```

IAM ROLES

- Grant temp privileges to a user
- Similar to IAM Users, however Roles need to be “Assumed”
- Restrict access to assume role using a trust policy
- Multiple users can share a role
- Can also be attached to services (e.g. Lambda function or EC2 instance that require access to another resource)

ROLE TRUST POLICY

- Defines who can assume the role
- Allows cross account access

```
aws iam list-roles
```


```
{
    "Roles": [
        {
            "Path": "/",
            "RoleName": "AdministratorRole",
            "RoleId": "AROAIWKUBFKX6GZI2ZYXS",
            "Arn": "arn:aws:iam::160367654759:role/AdministratorRole",
            "CreateDate": "2018-05-17T04:14:52Z",
            "AssumeRolePolicyDocument": {
                "Version": "2012-10-17",
                "Statement": [
                    {
                        "Effect": "Allow",
                        "Principal": {
                            "AWS": "arn:aws:iam::160367654759:root"
                        },
                        "Action": "sts:AssumeRole",
                        "Condition": {
                            "Bool": {
                                "aws:MultiFactorAuthPresent": "true"
                            }
                        }
                    }
                ]
            },
            "MaxSessionDuration": 3600
        },
```

Create role

1 2 3

Review

Provide the required information below and review this role before you create it.

Role name* Custom_Role

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description Custom Role

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

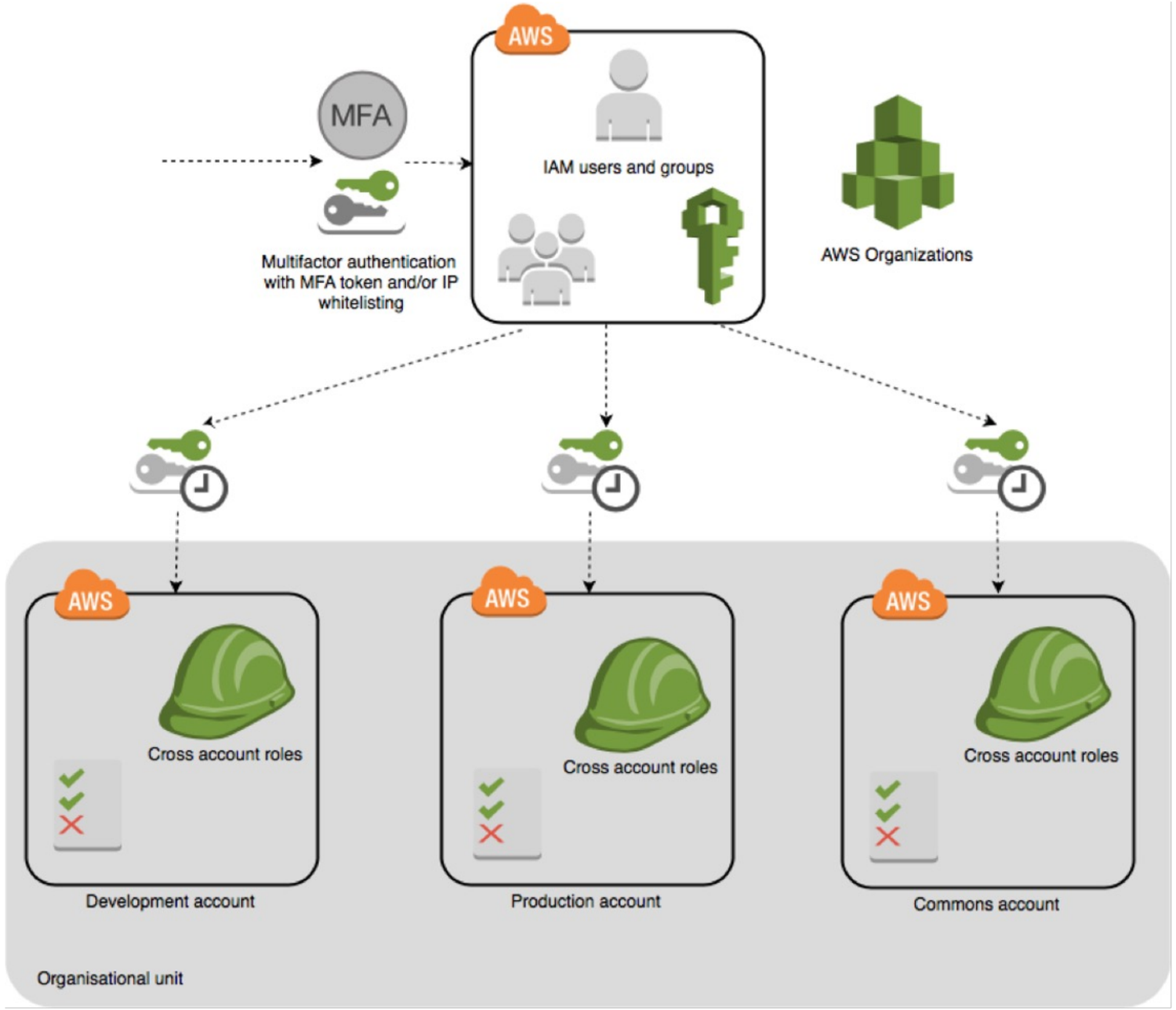
Trusted entities The account 496841392283

Policies Policies not attached

ASSUMING A ROLE

```
$ aws sts assume-role --role-arn
arn:aws:iam::496841392283:role/AssumeRoleForBackupAccount --role-
session-name test
```


```
{
    "Credentials": {
        "AccessKeyId": "ASIAJGWA46YDSDZ76AAQ",
        "SecretAccessKey": "FdvQm4CEUIpmQw8zQ373W7gLL56FXP4jfcqpaWMP",
        "SessionToken": "FQoDYXdzECYaDDmMYlVMusjWpVgk+yLoARLweP/27NvbhAzz/LFrSEjKHmMvdAsxEN9QY2LKO9f46kJzlq5M+Jg9gUFdceMkC4
YYlTLZHhObA6JTe+rUykA61KTv9hkEaS0sbaEdu4ckJLh/UvqLcvs1IbCtawtn3A2birP/rc0jqYCKJioJkzXexzqcHIcYABLtB89mGyDMvesrTdsJAf27cZeSc
5wbwpIID+ZMMQV9Gz+3kwA/tdQfURT5PswEjFlPOwWP7jSQYz+hkzb+W5Pkf0PijbgauR0SiJT4sJSGoxuUzC5ZEeuzwpnY0Kv0OZnLTOTWFUUfKWgQJhcB00ko
xJ6W2gU=",
        "Expiration": "2018-07-11T06:01:56Z"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAIJZQ7VSQY6SXEWC2K:test",
        "Arn": "arn:aws:sts::496841392283:assumed-role/AssumeRoleForBackupAccount/test"
    }
}
```


AWS
MFA
IAM users and groups
Multifactor authentication with MFA token and/or IP whitelisting
AWS Organizations
AWS
Cross account roles
Development account
AWS
Cross account roles
Production account
AWS
Cross account roles
Commons account
Organisational unit

HYBRID CLOUD

- Connecting Cloud with On Prem Infra/Services
- Could be part SaaS + On Prem, IaaS + SaaS + On Prem, or a variation

HYBRID CLOUD

AWS

ACTIVE DIRECTORY CONNECTOR

Directory gateway allowing directory requests to be redirected to on-prem Microsoft Active Directory

AWS DIRECTORY SERVICES FOR MICROSOFT AD

An actual Microsoft Windows Server AD managed by AWS in the AWS Cloud

FEDERATED

Federated Authentication

HYBRID CLOUD

AZURE AD

PASSWORD HASH SYNC (PHS)

Upload user accounts and password hashes into Azure AD

PASS THRU AUTHENTICATION (PTA)

Azure forwards the users login credentials to on-prem AD for authentication

FEDERATED

ADFS deployment

ATTACKING CLOUD SERVICES

Shared Security Responsibility

CLOUD PROVIDER

- Responsible for security of the cloud, e.g.
- Hardware, Software, Storage, etc.

CUSTOMER

- Responsible for security in the cloud, e.g.
- Access, Data, Apps, OS, Network, VM configs

HIGH RISK ISSUES

- MISCONFIGURED TRUST
- CONFUSED DEPUTIES
- PUCLICLY EXPOSED SERVICES
- SECRETS IN CODE REPOS
- HYBRID CLOUD WEAKNESSES

MISCONFIGURED TRUST

ROLES

- Anonymous trusted entity configured for AWS Roles
- This allows any AWS account who knows the ARN of the role to assume role

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

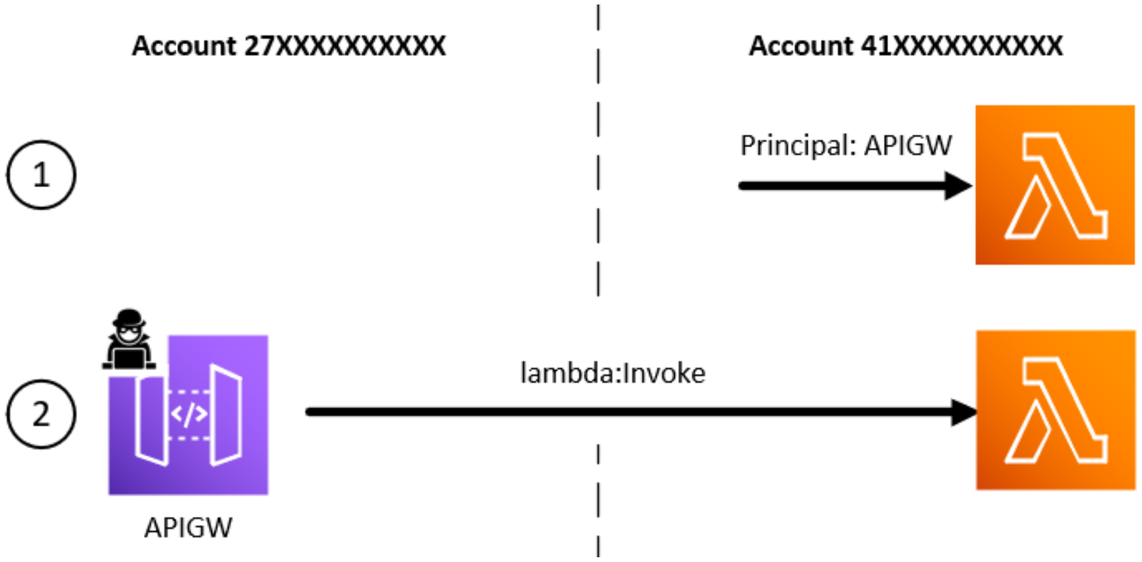
Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

MISCONFIGURED TRUST

SERVICE ROLES

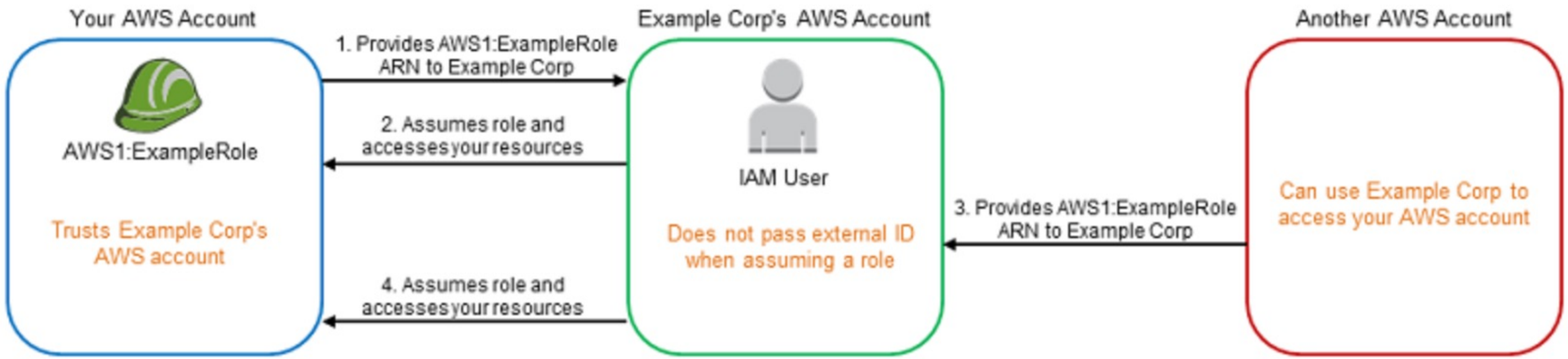
- Services that have roles attached could have to specifying the intended account in the trust policy
- This allows any AWS account who knows the ARN of the role to assume role



https://sra.io/blog/aws-iam-exploitation/

CONFUSED DEPUTIES

- Coercing a more-privileged entity to perform an action on your behalf
- CSRF is the equivalent in Web Applications
- E.g. Using an EC2 instance's role to access a resource which your role cannot access



ASSESSING IAM PERMISSIONS

- MANUALLY CHECK EACH USER, GROUP & ROLE IN IAM
- USE THE AWS CLI:
- `for i in `aws iam list-users --output text | awk '{print $7}' | awk 'NF'`; do (echo "Inline Policies for $i"; aws iam list-user-policies --user-name $i; echo "Managed Policies for $i"; aws iam list-attached-user-policies --user-name $i); done`
- USE PUBLICLY AVAILABLE TOOLS (RHINO SECURITY'S PACU, NCC GROUP'S SCOUT SUITE, ETC.)

IAM LEAST PRIVILEGES

GET ALL INLINE & MANAGED POLICIES ASSOCIATED WITH ALL IAM USERS

- `$ for i in `aws iam list-users --output text | awk '{print $7}' | awk 'NF'`; do (echo "Inline Policies for $i"; aws iam list-user-policies --user-name $i; echo "Managed Policies for $i"; aws iam list-attached-user-policies --user-name $i); done`

GET ALL INLINE & MANAGED POLICIES ASSOCIATED WITH ALL IAM GROUPS

- `$ for i in `aws iam list-groups --query 'Groups[*].{GroupName:GroupName}' --output text`; do (echo "Inline Policies for $i"; aws iam list-group-policies --group-name $i; echo "Managed Policies for $i"; aws iam list-attached-group-policies --group-name $i); done`

AWS IAM EXPLOITATION TOOL - PACU

```
  backdoor_assume_role
  privesc_scan

[Category: logging_monitoring]

  dl_cloudtrail_event_history
  disrupt_monitoring
  dl_cloudwatch_logs
  enum_monitoring

[Category: persistence]

  backdoor_users_password
  backdoor_users_keys

[Category: post_exploitation]

  cloudtrail_csv_injection
  add_ec2_startup_sh_script
  backdoor_ec2_sec_groups
  sysman_ec2_rce
  download_lightsail_ssh_keys

[Category: recon_enum_no_keys]

  s3_finder

[Category: recon_enum_with_keys]

  inspector_report_fetcher
  enum_ebs_volumes_snapshots
  download_ec2_userdata
  enum_ec2_termination_protection
  get_credential_report
  enum_ec2
  confirm_permissions
  enum_glue
  enum_codebuild
  enum_lightsail
  enum_users_roles_policies_groups
  s3_bucket_dump
  enum_lambda
  enum_elb_logging

Pacu (TestSession:TestUser) >
```

IAM PERMISSIONS THAT MAY ALLOW PRIVILEGE ESCALATION

- iam:CreatePolicyVersion
  - Allows creation of new policy version and setting it as default, giving users elevated permissions
- iam:CreateAccessKey (aws iam create-access-key -user-name target_user)
  - Allows creation of IAM keys for other users
- iam:CreateLoginProfile
  - Allows creation of new user's profile and setting their credentials
- iam:UpdateLoginProfile
  - Allows modification of user's profiles

More info and write-up https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/ &

https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation-part-2/

PUBLICLY EXPOSED RESOURCES

- Public S3 Buckets, DB Snapshots, AMIs/VM Images, KMS Keys, etc.

Twitch says no passwords or login credentials leaked in massive breach

The company is still investigating a massive hack that drew headlines two weeks ago.

Written by **Jonathan Greig**, Staff Writer
on October 16, 2021 | Topic: **Security**

Twitch has come out with a new statement denying the severity of the breach that drew headlines earlier this month.

The gaming platform reiterated that the incident was caused by a "server configuration change that allowed improper access by an unauthorized third party."

ZDNET RECOMMENDS

The best password manager: Business and personal use

RELATED

Shure MV7 review: An 'almost perfect' hybrid mic for podcasters and streamers

You can invest in PvP International, the web's first true online hub for gamers -- new investments close April 8th

6 AUG 2021 NEWS

Millions of Senior Citizens' Personal Data Exposed by Misconfiguration

James Coker Reporter, Infosecurity Magazine
Follow @ReporterCoker

Millions of senior citizens in North America have had their personal information compromised following a breach at senior care review website SeniorAdvisor, according to WizCase.

The researchers, led by Ata Hakcil, discovered a misconfigured Amazon S3

Related to This Story

British Council Students' Data Exposed in Major Breach

Interview: Mijo Soldin, Director Operator Strategy and Partnerships, Infobip

Utah COVID-19 testing service exposes 50,000 patients' photo IDs, personal info on the web

A coronavirus testing company in Utah exposed more than 50,000 patients' scanned IDs and thousands of COVID-19 test results.

1,000 GB of local government data exposed by Massachusetts software company

A group of ethical researchers found over 80 misconfigured Amazon S3 buckets holding data related to about 100 municipalities across the Northeast.

Written by **Jonathan Greig**, Staff Writer
on July 22, 2021 | Topic: **Government: US**

More than 1,000 GB of data and over 1.6 million files from dozens of municipalities in the US were left exposed, according to a new report from a

RELATED

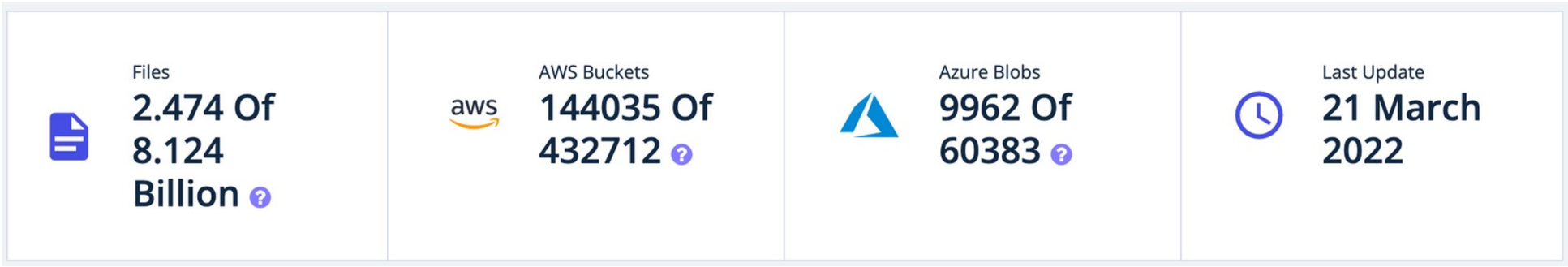
Yes, the cloud is still safe despite the AWS outage - if you learn from failure

Best US Bank credit card

PUBLIC S3 BUCKETS

https://github.com/nagwww/s3-leaks

https://buckets.grayhatwarfare.com/



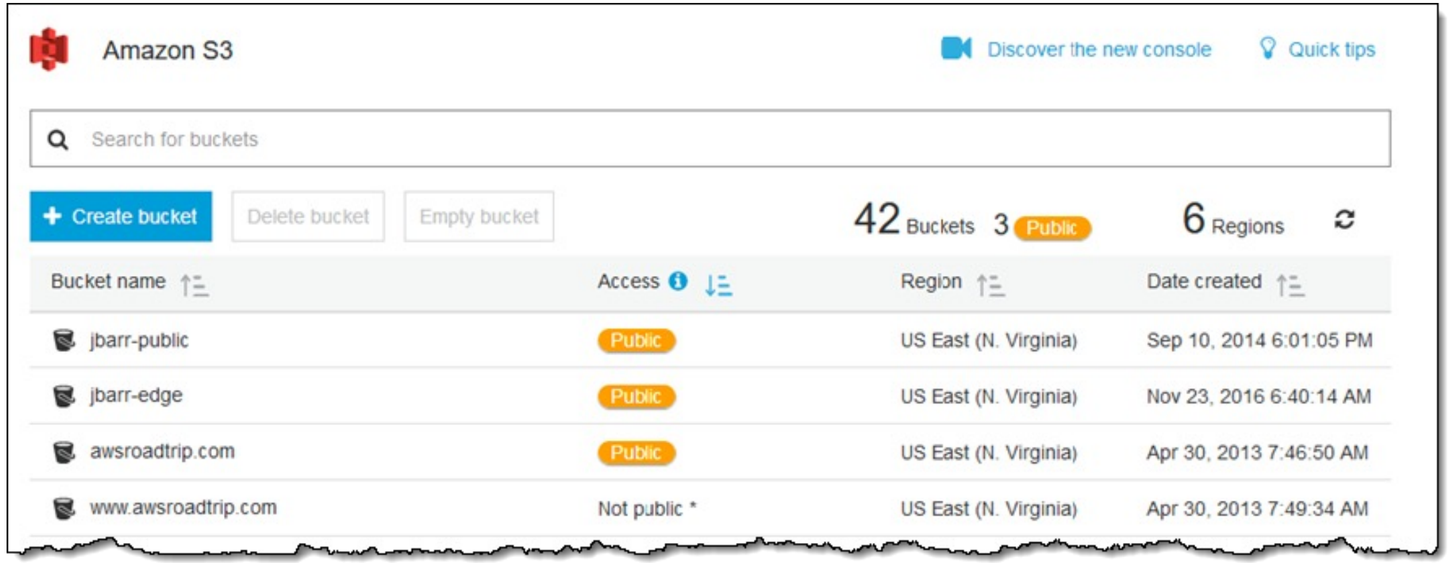
PUBLIC S3 BUCKETS

Check for public buckets in all environments

Using the CLI:

```
for i in `aws s3 ls | awk '{print $3}'`; do (echo "Policy for $i"; aws s3api get-bucket-policy --bucket $i --output text); done
```

•Using the Console:



PUBLIC S3 BUCKETS

```
$ s3scanner scan --buckets-file bucket-names.txt
summer.starbucks.com | bucket_exists | AuthUsers: [], AllUsers: [Read]
placewise | bucket_exists | AuthUsers: [], AllUsers: []
hype-prod | bucket_exists | AuthUsers: [], AllUsers: []
csbd.sony.com | bucket_not_exist
udemy-web-upload-bucket | bucket_exists | AuthUsers: [], AllUsers: []
mdsp-test | bucket_not_exist
pendo | bucket_exists | AuthUsers: [], AllUsers: [Read, ReadACP]
rzeczoznawca | bucket_exists | AuthUsers: [], AllUsers: [Read]
red-dev | bucket_exists | AuthUsers: [], AllUsers: []
allinoneseo | bucket_exists | AuthUsers: [], AllUsers: [Read]
save-song | bucket_not_exist
gandcfabcon | bucket_not_exist
deveo | bucket_exists | AuthUsers: [], AllUsers: [Read]
appshack | bucket_exists | AuthUsers: [], AllUsers: [Read]
woo-staging | bucket_exists | AuthUsers: [], AllUsers: [Read, ReadACP]
checkon | bucket_not_exist
caspar-staging | bucket_exists | AuthUsers: [], AllUsers: [Read]
pinnacle-dev | bucket_exists | AuthUsers: [], AllUsers: [Read, Write, ReadACP, WriteACP]
lumaforge | bucket_exists | AuthUsers: [], AllUsers: [Read, ReadACP]
rodekors | bucket_exists | AuthUsers: [], AllUsers: [Read]
mustafa | bucket_exists | AuthUsers: [], AllUsers: [FullControl]
dev-place | bucket_not_exist
sioux | bucket_exists | AuthUsers: [], AllUsers: [ReadACP]
vtc-test | bucket_exists | AuthUsers: [], AllUsers: [Read]
$
```

https://github.com/sa7mon/S3Scanner

SECRETS IN CODE REPOS

- Accidental Exposure of sensitive data
- Recent Data Exposures:
  - Administrator credentials to sensitive systems
  - Personal data of millions of users
  - Sensitive information about IT systems
  - Proprietary code
  - Terabytes of top secret government data
  - Master access keys for AWS Key Management system,
  - Plaintext databases
  - Gigabytes of financial information

PUBLIC EC2 IMAGES

```
$ aws ec2 describe-images

…
"Architecture": "x86_64",
"CreationDate": "2012-11-08T23:00:14.000Z",
"ImageId": "aki-0b861131",
"ImageLocation": "ubuntu-ap-southeast-2/kernels/ubuntu-lucid-amd64-linux-image-
2.6.32-34-ec2-v-2.6.32-347.53-kernel.img.manifest.xml",
"ImageType": "kernel",
"Public": true,
"OwnerId": "099720109477",
"State": "available",
"BlockDeviceMappings": [],

…
```

INTERNET ACCESSIBLE UNAUTHENTICATED DATABASE SNAPSHOTS

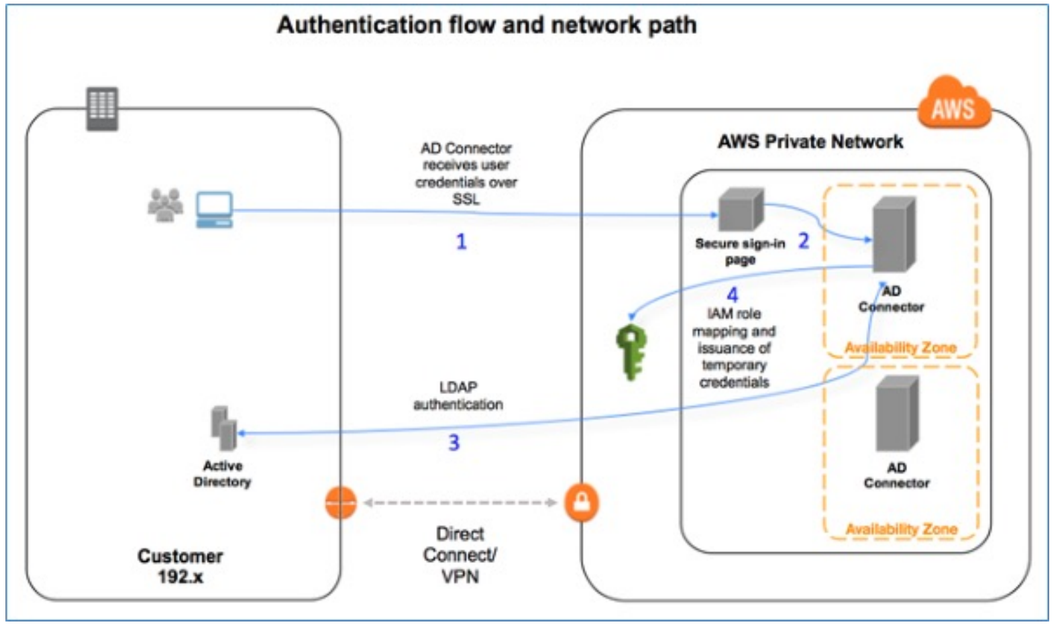
```
$ aws rds describe-db-snapshot-attributes --region us-east-1 --db-snapshot-identifier prod-sql-snapshot --query 'DBSnapshotAttributesResult.DBSnapshotAttributes'

$ { "AttributeName": "restore", "AttributeValues": [ "all" ] }
```

HYBRID CLOUD

ATTACKING HYBRID + MULTI CLOUD ENVIRONMENTS

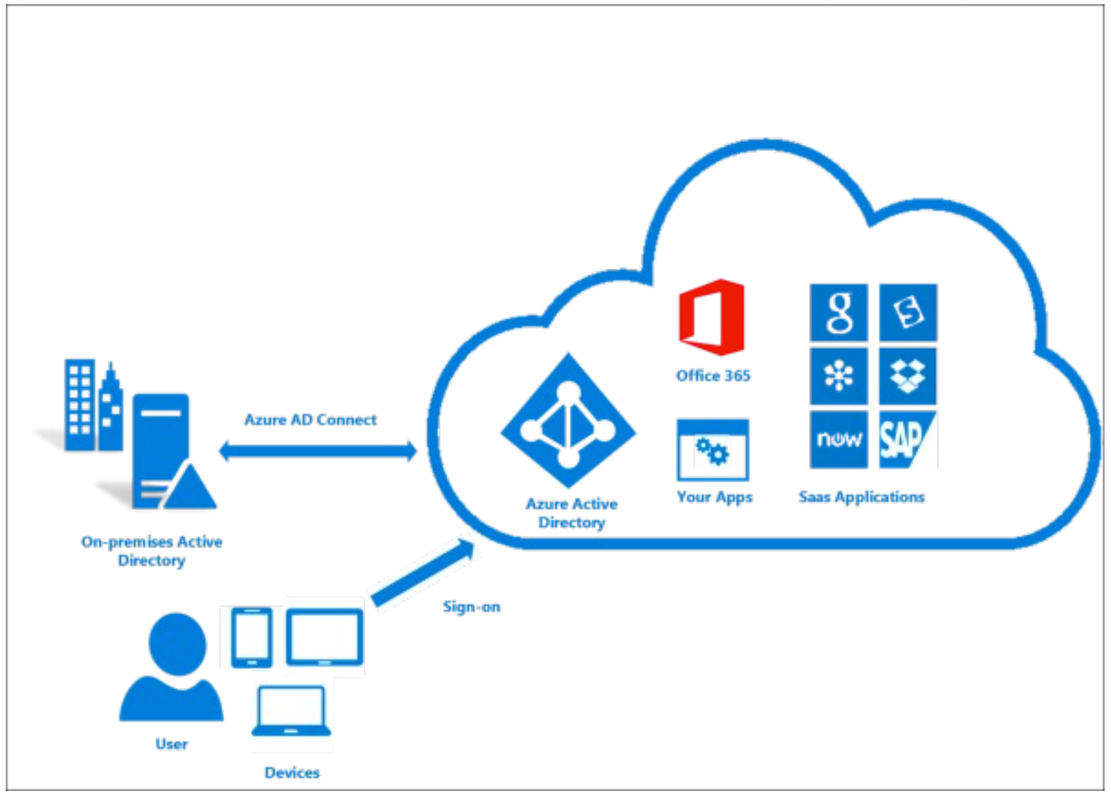
AMAZON AD CONNECTOR

- Acts as an Authentication Proxy for On Prem AD
- On Authentication, the AD Connector creates AWS IAM tokens for the roles mapped to the AD account
- Targeting the AD Connector environment when attacking an AWS environment may provide access to those temporary tokens which would allow impersonating the user



AZURE AD CONNECT

- Password Hash Sync (PHS) - Upload user accounts and password hashes into Azure AD
- Pass Thru Authentication (PTA) - Azure forwards the users login credentials to in prem AD for authentication
- Azure AD Seamless Single Sign on



ATTACKING HYBRID CLOUD - SUMMARY

- Once AD option in use is identified, path towards admin accounts needs to be determined
- Primary focus is getting privileged access
- If access to Cloud services is available, going after admin users, groups, roles may be useful
- Enumeration of AD & IAM may reveal privilege escalation scenarios
- Azure AD Domain Services allows several options to sync with on prem AD, some publicly know ways to obtain password hashes
- Compromising a cloud VM/instance could allow compromise of any associated on-prem roles & accounts and therefore on-prem resources

SECURE CONFIG

- Use hardened and approved OS images, templates, & access policies
- IAM - Use the principal of least privilege

VALIDATION/ATTESTATION DURING BUILD PROCESS

- Scan/Identify and remediate prior to deployment
- Integrated into the build pipeline, or manually initiated
- Auto remediation is also available but can introduce challenges - using a phased approach could be easier, esp. for large scale multi developer teams in multi account environments

AUDITING

- Perform regular security audits of your cloud environments & permissions

Lessons Learnt

PRINCIPAL OF LEAST PRIVILEGE

- Limit Privileged Host Access
- No remote management access (e.g. SSH or RDP) to the container

NETWORK SECURITY

- Use Firewalls and Network Filtering
- Limit Traffic between host and containers
- Reduces Network Access of compromised instances/containers

MONITORING

- Integration of Logs (Cloud/On-Prem/Container)
- Logging, hardware & network management is handled outside of the account/container/env.

TIME LIMIT

- By forcing containers to be short lived allows them to go through deployment checks for new vulnerabilities

Lessons Learnt (Container Environments)

SUMMARY

- High complexity of IAM & Hybrid Cloud environments can lead to high likelihood of misconfigurations
- Hybrid Cloud environments are not well understood, and they get complex in larger organisations with multi cloud and SaaS providers
- Each Cloud provider have their own requirements and ways to sync with on prem
- Harden the environments & Perform Regular Auditing and Security Testing
  - Various guides & tools/resources available to handle config management, monitoring, detection, and auto correction
  - Limit IAM permissions using service control policies and permissions boundaries
- MFA Everything
- Monitoring & detection should be implemented
- Have a Response Plan

RESOURCES/CREDITS

- Rhino Security Labs - https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
- NCC Labs - https://www.owasp.org/images/c/cc/AWS_Security_-_Staying_on_Top_of_the_Cloud.pdf
- Adam Chester, https://blog.xpnsec.com/azuread-connect-for-redteam/
- Michael Grafnetter, https://www.dsinternals.com/en/impersonating-office-365-users-mimikatz/
- Sean Metcalf, https://www.trimarcsecurity.com/single-post/hacking-the-cloud, DEF CON Safe Mode - Sean Metcalf - Hacking the Hybrid Cloud
- https://sra.io/blog/aws-iam-exploitation/
- https://docs.aws.amazon.com/cli/latest/index.html
- Tools for Auditing AWS/Azure Permissions
  - SkyArk - https://github.com/cyberark/SkyArk
  - Rhino Security's AWS_Escalate - https://github.com/RhinoSecurityLabs/Security-Research/blob/master/tools/aws-pentest-tools/aws_escalate.py
  - Rhino Security's Pacu - https://github.com/RhinoSecurityLabs/pacu
  - NCC Group's Pmapper - https://github.com/nccgroup/PMapper
  - NCC Group's ScoutSuite - https://github.com/nccgroup/ScoutSuite
  - AWS-IAM-Permissions-Scanner - https://github.com/nemo-wq/AWS-IAM-Permissions-Scanner