





# AWS IAM Privilege Escalation Methods







Pralhad Chaskar (@c0d3xploit)

# Amazon Web Services





## Compute

-  **EC2**  
Virtual Servers in the Cloud
-  **EC2 Container Service**  
Run and Manage Docker Containers
-  **Elastic Beanstalk**  
Run and Manage Web Apps
-  **Lambda**  
Run Code in Response to Events




## Storage & Content Delivery

-  **S3**  
Scalable Storage in the Cloud
-  **CloudFront**  
Global Content Delivery Network
-  **Elastic File System** **PREVIEW**  
Fully Managed File System for EC2
-  **Glacier**  
Archive Storage in the Cloud
-  **Import/Export Snowball**  
Large Scale Data Transport
-  **Storage Gateway**  
Integrates On-Premises IT Environments with Cloud Storage


## Database

-  **RDS**  
Managed Relational Database Service
-  **DynamoDB**  
Predictable and Scalable NoSQL Data Store
-  **ElastiCache**  
In-Memory Cache
-  **Redshift**  
Managed Petabyte-Scale Data Warehouse Service








## Networking

-  **VPC**  
Isolated Cloud Resources
-  **Direct Connect**  
Dedicated Network Connection to AWS
-  **Route 53**  
Scalable DNS and Domain Name Registration





## Developer Tools

-  **CodeCommit**  
Store Code in Private Git Repositories
-  **CodeDeploy**  
Automate Code Deployments
-  **CodePipeline**  
Release Software using Continuous Delivery





## Management Tools

-  **CloudWatch**  
Monitor Resources and Applications
-  **CloudFormation**  
Create and Manage Resources with Templates
-  **CloudTrail**  
Track User Activity and API Usage
-  **Config**  
Track Resource Inventory and Changes
-  **OpsWorks**  
Automate Operations with Chef
-  **Service Catalog**  
Create and Use Standardized Products
-  **Trusted Advisor**  
Optimize Performance and Security

## Security & Identity

-  **Identity & Access Management**  
Manage User Access and Encryption Keys
-  **Directory Service**  
Host and Manage Active Directory
-  **Inspector** **PREVIEW**  
Analyze Application Security
-  **WAF**  
Filter Malicious Web Traffic






## Analytics

-  **EMR**  
Managed Hadoop Framework
-  **Data Pipeline**  
Orchestration for Data-Driven Workflows
-  **Elasticsearch Service**  
Run and Scale Elasticsearch Clusters
-  **Kinesis**  
Work with Real-time Streaming data








## Internet of Things

-  **AWS IoT** **BETA**  
Connect Devices to the cloud




## Mobile Services

-  **Mobile Hub** **BETA**  
Build, Test, and Monitor Mobile apps
-  **Cognito**  
User Identity and App Data Synchronization
-  **Device Farm**  
Test Android, Fire OS, and iOS apps on real devices in the Cloud
-  **Mobile Analytics**  
Collect, View and Export App Analytics
-  **SNS**  
Push Notification Service

## Application Services

-  **API Gateway**  
Build, Deploy and Manage APIs
-  **AppStream**  
Low Latency Application Streaming
-  **CloudSearch**  
Managed Search Service
-  **Elastic Transcoder**  
Easy-to-use Scalable Media Transcoding
-  **SES**  
Email Sending Service
-  **SQS**  
Message Queue Service
-  **SWF**  
Workflow Service for Coordinating Application Components


## Enterprise Applications

-  **WorkSpaces**  
Desktops in the Cloud
-  **WorkDocs**  
Secure Enterprise Storage and Sharing Service
-  **WorkMail** **PREVIEW**  
Secure Email and Calendaring Service

# Recap of AWS

- ACCESS\_KEYS → Identifier of the user in account
  - SECRET\_ACCESS\_KEY → Password needed to authenticate
  - SESSION\_TOKEN → Security Token
- 
- AWS CLI → Console client written in python that allows a user to interact with the different services offered by AWS


# Permission Policies

 AdministratorAccess

Policy summary

{ } JSON

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "*",
7       "Resource": "*"
8     }
9   ]
10 }
```

 AmazonEC2ReadOnlyAccess

Policy summary

{ } JSON

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:Describe*",
7       "Resource": "*"
8     },
9     {
10      "Effect": "Allow",
11      "Action": "elasticloadbalancing:Describe*",
12      "Resource": "*"
13    }
14  ]
15 }
```

# Privilege Escalation in the cloud

- Misconfiguration of identity and access management (IAM) policies
- Manipulation of APIs
- Cloud provider vulnerabilities

# For Auditors/Pentesters/BlueTeamer

Take one user per role in order to check Privilege Escalation possibility and feed the ACCESS\_KEYS, SECRET\_ACCESS\_KEY, SESSION\_TOKEN to below demo'ed tools.

# AWS\_ESCALATE.py

```
root@kali:~/Desktop/cloudgoat# python3 aws_escalate.py
No AWS CLI profile passed in, choose one below or rerun the script using the -p/--profile argument:
[0] cloudgoat
[1] raynor
Choose a profile (Ctrl+C to exit): 1
Enumerating permissions for 3 users...
  cloudgoat... done!
  raynor... done!
  root-accnt... done!

Enumerating permissions for 6 roles...
  AWSServiceRoleForAmazonGuardDuty... done!
  AWSServiceRoleForAmazonInspector... done!
  AWSServiceRoleForElasticLoadBalancing... done!
  AWSServiceRoleForRDS... done!
  AWSServiceRoleForSupport... done!
  AWSServiceRoleForTrustedAdvisor... done!

User: cloudgoat
  Already an admin!

User: raynor
  CONFIRMED: SetExistingDefaultPolicyVersion

User: root-accnt
  Already an admin!

Role: AWSServiceRoleForAmazonGuardDuty
  No methods possible.

Role: AWSServiceRoleForAmazonInspector
  No methods possible.
```

# PACU

- Pacu is an open source AWS exploitation framework, designed for offensive security testing against cloud environments.

Below are some capabilities/modules

- RECON\_UNAUTH
- ENUM
- **ESCALATE** (run iam\_\_privesc\_scan)
- LATERAL\_MOVE
- EXPLOIT
- PERSIST
- EXFIL
- EVADE



```
Pacu > run iam_privesc_scan
```

```
Running module iam__privesc_scan...
[iam__privesc_scan] Escalation methods for current role:
[iam__privesc_scan]   CONFIRMED: CreateNewPolicyVersion
[iam__privesc_scan]   CONFIRMED: SetExistingDefaultPolicyVersion
[iam__privesc_scan]   CONFIRMED: CreateAccessKey
[iam__privesc_scan]   CONFIRMED: CreateLoginProfile
[iam__privesc_scan]   CONFIRMED: UpdateLoginProfile
[iam__privesc_scan]   CONFIRMED: AttachRolePolicy
[iam__privesc_scan]   CONFIRMED: PutRolePolicy
[iam__privesc_scan]   CONFIRMED: PassExistingRoleToNewLambdaThenInvoke
[iam__privesc_scan]   CONFIRMED: PassExistingRoleToNewLambdaThenTriggerWithNewDynamo
[iam__privesc_scan]   CONFIRMED: PassExistingRoleToNewLambdaThenTriggerWithExistingDynamo
[iam__privesc_scan]   CONFIRMED: PassExistingRoleToNewCloudFormation
[iam__privesc_scan]   CONFIRMED: EditExistingLambdaFunctionWithRole
[iam__privesc_scan] Attempting confirmed privilege escalation methods...
```

```
[iam__privesc_scan]      2 valid user-attached policy(ies) found...
```

```
[iam__privesc_scan]      [0] nonprod-ServerlessAccess
```

```
[iam__privesc_scan] [1] developer_NonProd_Params
```

```
[iam_privesc_scan]      Choose an option: 1
```

```
[iam__privesc_scan]    Privilege escalation successful using method CreateNewPolicyVersion!
```

The current user is now an administrator ("\*" permissions on "\*" resources).

# Demo



# References

- [https://github.com/RhinoSecurityLabs/Cloud-Security-Research/tree/master/AWS/aws\\_escalate](https://github.com/RhinoSecurityLabs/Cloud-Security-Research/tree/master/AWS/aws_escalate)
- <https://github.com/RhinoSecurityLabs/pacu/wiki/Module-Details>
- <https://github.com/RhinoSecurityLabs/AWS-IAM-Privilege-Escalation>

A large, fluffy white question mark is the central focus of the image, set against a clear blue sky with scattered wispy clouds. Below the main question mark, there is a smaller, solid white cloud.

THANK YOU

Any Questions ?