Cloud Operational Security

## Summary

## This lab looks at controlling access to AWS EC2 instances without using SSH.

## Tools/Resources

AWS account

## Tasks

* Create IAM role for SSM access to EC2 instance
* Create instance profile for new role
* Create Security Group with no public access
* Create EC2 launch template
* Launch manager EC2 instance without keypair
* Connect to instance with System Manager and issue the following commands:

date

TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl- seconds: 21600"`

echo $TOKEN

curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document

## Submission

Upload to Canvas screenshot of System Manager session.

## Walkthrough

<https://docs.aws.amazon.com/systems-manager/latest/userguide/getting-started-create-iam-instance-profile.html#create-iam-instance-profile-ssn-only>

KMS key gen first

**MySessionManagerRole**

**Attach to instance**

<https://us-east-2.console.aws.amazon.com/systems-manager/session-manager/start-session?region=us-east-2>

1. Create IAM role

Pick AWS service, Use case=systems manager, click next.

Fill in name (IT666\_SSM\_managed), select AmazonSSMManagedInstanceCore, “create role”

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The result is anything with this role will allow SSM interactions.

A screenshot of a computer program

Description automatically generated

1. Create an instance profile

[cloudshell-user@ip-10-134-94-249 ~]$ aws iam create-instance-profile --instance-profile-name it666-profile1

{

"InstanceProfile": {

"Path": "/",

"InstanceProfileName": "it666-profile1",

"InstanceProfileId": "AIPA3PIY6PEX3R2B5XJIX",

"Arn": "arn:aws:iam::788715698479:instance-profile/it666-profile1",

"CreateDate": "2024-08-12T20:08:35+00:00",

"Roles": []

}

}

[cloudshell-user@ip-10-134-94-249 ~]$ aws iam add-role-to-instance-profile --instance-profile-name it666-profile1 --role-name it666\_ssm\_managed

1. Create a security group that only allows private traffic

A screenshot of a computer

Description automatically generated

1. EC2 launch template (OK to reuse template from SSH lab)

My existing template is: Name=SessionManagerOnlyAccess Id=lt-0857f82c08801d8d9

[cloudshell-user ~]$ aws ec2 describe-launch-templates | jq -r '.LaunchTemplates[].LaunchTemplateName'

Docker

ProjectExample

CTFD

Kali-RDP

it666-kmh722-ssh

IT666\_SSH\_basic\_AMI

Blockchain

SessionManagerOnlyAccess

[cloudshell-user ~]$ aws ec2 describe-launch-templates --launch-template-names SessionManagerOnlyAccess

{

"LaunchTemplates": [

{

"LaunchTemplateId": "lt-0857f82c08801d8d9",

"LaunchTemplateName": "SessionManagerOnlyAccess",

"CreateTime": "2024-08-09T18:46:40+00:00",

"CreatedBy": "arn:aws:iam::788715698479:user/Ken",

"DefaultVersionNumber": 1,

"LatestVersionNumber": 5

}

]

}

[cloudshell-user ~]$ aws ec2 describe-launch-template-versions --launch-template-id lt-0857f82c08801d8d9 --versions 5

{

"LaunchTemplateVersions": [

{

"LaunchTemplateId": "lt-0857f82c08801d8d9",

"LaunchTemplateName": "SessionManagerOnlyAccess",

"VersionNumber": 5,

"CreateTime": "2024-08-12T00:00:28+00:00",

"CreatedBy": "arn:aws:iam::788715698479:user/Ken",

"DefaultVersion": false,

"LaunchTemplateData": {

"NetworkInterfaces": [

{

"AssociatePublicIpAddress": true,

"DeviceIndex": 0,

"Groups": [

"sg-09478a8bbd1e1e03d"

],

"SubnetId": "subnet-c262918f"

}

],

"ImageId": "ami-05c3dc660cb6907f0",

"InstanceType": "t2.micro",

"UserData": "",

"MetadataOptions": {

"HttpTokens": "required",

"HttpPutResponseHopLimit": 2,

"HttpEndpoint": "enabled"

}

}

}

]

1. Launch template
   1. no keypair
   2. your private local only sg
   3. advanced details: your IAM instance profile, no user-data
2. EC2 home page, select running instance, click Connect
3. System manager -> session managerA screenshot of a computer

   Description automatically generated
4. Get system info

A screenshot of a computer

Description automatically generated

Capture the SSM session output text

sh-5.2$ date

Wed Oct 23 14:02:22 UTC 2024sh-5.2$

sh-5.2$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 56 100 56 0 0 14583 0 --:--:-- --:--:-- --:--:-- 18666

sh-5.2$

sh-5.2$ echo $TOKEN

AQAEAH\_gQFAaD-0Ga1FaSmeZveqMALikY52qmA8GppDDISTEKuuJLA==

sh-5.2$

sh-5.2$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document

{

"accountId" : "788715698479",

"architecture" : "x86\_64",

"availabilityZone" : "us-east-2c",

"billingProducts" : null,

"devpayProductCodes" : null,

"marketplaceProductCodes" : null,

"imageId" : "ami-05c3dc660cb6907f0",

"instanceId" : "i-09b8308803a17ca08",

"instanceType" : "t2.micro",

"kernelId" : null,

"pendingTime" : "2024-10-23T13:45:29Z",

"privateIp" : "172.31.36.249",

"ramdiskId" : null,

"region" : "us-east-2",

"version" : "2017-09-30"

}sh-5.2$

## sh-5.2$ Additional Thoughts

Open ports? Netstat -plnt

What connections are open / listening? ss -t / ss -lt

DD commands: <https://www.tecmint.com/ss-command-examples-in-linux/>

Do we allow this system to create another?

How does …