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 PACP 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

from IP 18.192.239.172 to S3

Discovery of IAM Role Details

Retrieved Instance Profile ARN and ID

Temporary IAM Credentials Theft

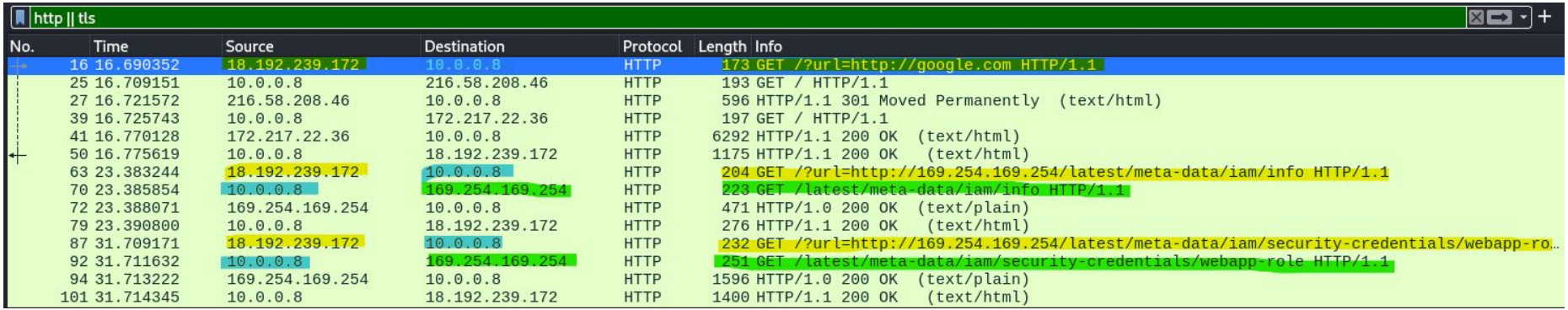
Extracted temporary credentials (AccessKeyId, SecretAccessKey, Token)

Exfiltration of Sensitive Files

Used stolen credentials to download sensitive files

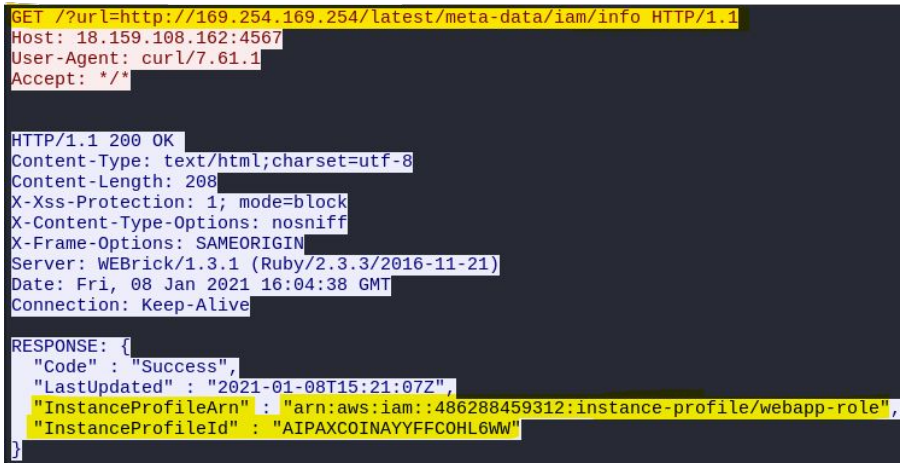
Unauthorized Access

- **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.



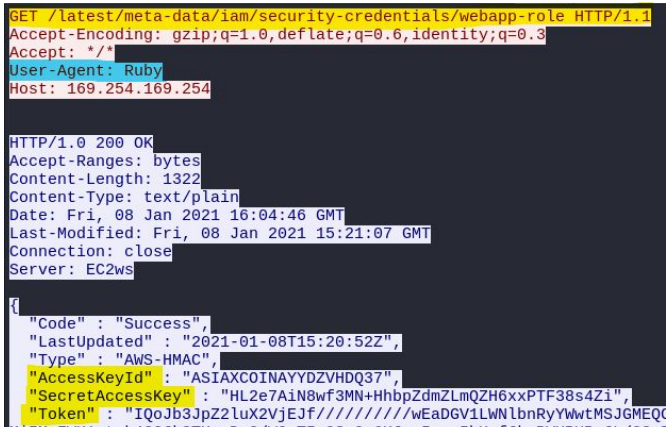
Discovery of IAM Role Information

- **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



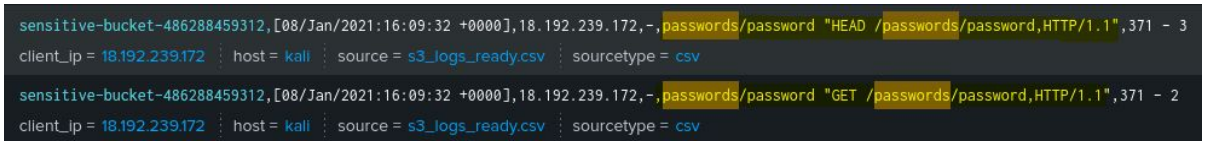
Retrieval of Temporary IAM Credentials

- **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.



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`



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