Blue Team Assessment Report

Testing Organization

Tester's Name

Jakub Jędrzejczak

Test Date

06/12/2024

Table of Contents

Introduction

1 Overview

Niniejszy raport dokumentuje dochodzenie przeprowadzone na koncie AWS przy użyciu dostarczonych kluczy dostępu. Celem było zidentyfikowanie użytkownika powiązanego z kluczami, znalezienie dodatkowych użytkowników, uzyskanie dostępu do poufnych informacji w zasobnikach S3 i pobranie poufnych plików. W ramach dochodzenia podjęto następujące kroki:

Konfiguracja AWS CLI z dostarczonymi kluczami dostępu.

-Badanie zagrożeń związanych z ujawnionymi kluczami dostępu.

-Identyfikacja użytkownika powiązanego z kluczami dostępu.

-Wykrycie innych użytkowników w systemie korzystających z dostarczonych kluczy.

-Uzyskanie dostępu i wylistowanie zawartości bucketów S3 w celu znalezienia poufnych informacji.

-Pobranie poufnych plików z zasobników S3.

Scope

The client, "Technician Blog", specified that the testing will occur only on a beta version of the website, located in a container made by “Docker.” The client forbids testing on the live site.

2 Out of Scope

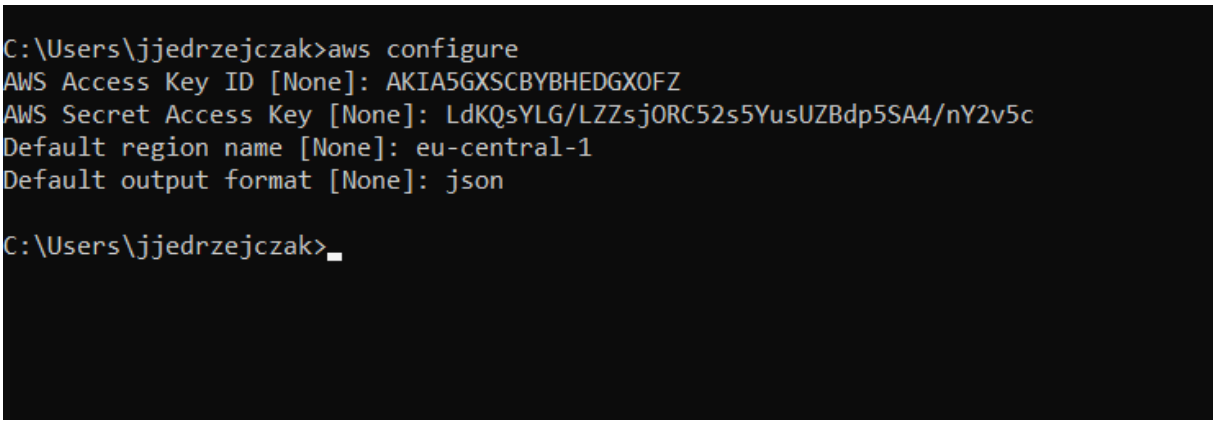
Szczegółowego badania innych usług AWS niezwiązanych bezpośrednio z udostępnionymi kluczami i bucketami S3.

Analiza potencjalnego wpływu lub środków zaradczych dla ujawnionych kluczy poza wstępnymi zaleceniami.

Obszernego przeglądu wszystkich zasad IAM i ról wykraczających poza bezpośrednią identyfikację użytkownika i działania podjęte przy użyciu dostarczonych kluczy.

Detailed Findings

1.



2.

Dlaczego Eksponowanie Kluczy Jest Niebezpieczne

1. Nieautoryzowany Dostęp:

Klucze mogą być wykorzystane przez osoby trzecie do nieautoryzowanego dostępu do zasobów AWS, co może prowadzić do ich modyfikacji, usuwania lub tworzenia nowych zasobów.

2. Zagrożenie Finansowe:

Nieautoryzowany użytkownik może generować zasoby, co prowadzi do nieprzewidzianych kosztów na koncie AWS.

3. Naruszenie Bezpieczeństwa Danych:

Dostęp do poufnych danych w S3 lub innych usługach AWS może prowadzić do poważnych naruszeń bezpieczeństwa i prywatności.

4.Naruszenie Przepisów:

Ujawnienie danych osobowych może prowadzić do naruszenia przepisów ochrony danych, co może skutkować karami i odpowiedzialnością prawną.

Przykłady Eksponowania Kluczy

1. Publiczne Repozytoria Kodów:

Klucze mogą być przypadkowo zamieszczone w publicznych repozytoriach GitHub, co jest częstą przyczyną ich eksponowania.

2. Logi i Zrzuty Ekranów:

Klucze mogą być zapisane w logach aplikacji lub zrzutach ekranów, które są następnie publicznie udostępniane.

3.Niewłaściwe Zarządzanie Kluczami:

Brak rotacji kluczy dostępu lub pozostawianie ich aktywnymi przez długi czas zwiększa ryzyko nieautoryzowanego użycia.

3.

Ben

```
C:\Users\jjedrzejczak>aws iam get-user
{
    "User": {
        "Path": "/",
        "UserName": "ben",
        "UserId": "AIDA5GXSCBYBI3QETGOSM",
        "Arn": "arn:aws:iam::907819486722:user/ben",
        "CreateDate": "2022-08-23T07:10:31+00:00",
        "Tags": [
            {
                "Key": "user",
                "Value": "cloud security project"
            }
        ]
    }
}


C:\Users\jjedrzejczak>
```

4.

```
C:\Users\jjedrzejczak>aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "ben",
            "UserId": "AIDA5GXSCBYBI3QETGOSM",
            "Arn": "arn:aws:iam::907819486722:user/ben",
            "CreateDate": "2022-08-23T07:10:31+00:00"
        },
        {
            "Path": "/",
            "UserName": "john",
            "UserId": "AIDA5GXSCBYBJDKIXHZKC",
            "Arn": "arn:aws:iam::907819486722:user/john",
            "CreateDate": "2022-08-23T07:11:51+00:00"
        },
        {
            "Path": "/",
            "UserName": "roman",
            "UserId": "AIDA5GXSCBYBBVKADT47C",
            "Arn": "arn:aws:iam::907819486722:user/roman",
            "CreateDate": "2022-08-23T07:12:54+00:00"
        },
        {
            "Path": "/",
            "UserName": "swaroop",
            "UserId": "AIDA5GXSCBYBLNS7DF2TJ",
            "Arn": "arn:aws:iam::907819486722:user/swaroop",
            "CreateDate": "2022-08-23T07:14:35+00:00"
        }
    ]
}
```

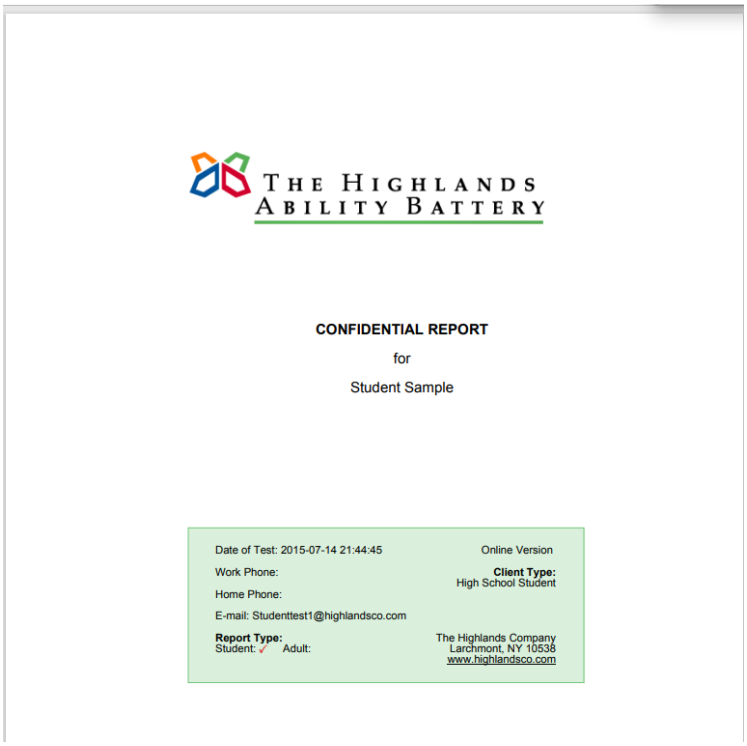
5.
```
C:\Users\jjedrzejczak>aws s3 ls
2022-08-23 09:16:45 cloudsecurityconfidential

C:\Users\jjedrzejczak>aws s3 ls s3://cloudsecurityconfidential
2022-08-23 17:30:32     713060 confidential_doc.pdf
```

6.
```
C:\Users\jjedrzejczak>aws s3 cp s3://cloudsecurityconfidential/confidential_doc.pdf .
download: s3://cloudsecurityconfidential/confidential_doc.pdf to .\confidential_doc.pdf

C:\Users\jjedrzejczak>
```

```
06/12/2024  09:08 AM                 0 aws
06/12/2024  09:12 AM               175 batch.bat
05/20/2024  03:21 PM    <DIR>          Cisco Packet Tracer 8.2.2
08/23/2022  05:30 PM           713,060 confidential_doc.pdf
10/17/2022  09:44 AM    <DIR>          Contacts
```



THE HIGHLANDS ABILITY BATTERY

CONFIDENTIAL REPORT

for

Student Sample

Date of Test: 2015-07-14 21:44:45 — Online Version

Work Phone:

Home Phone:

E-mail: Studenttest1@highlandsco.com

Client Type: High School Student

Report Type: Student: ✓ Adult:

The Highlands Company
Larchmont, NY 10538
www.highlandsco.com

7.

Summary

Dochodzenie potwierdziło, że dostarczone klucze dostępu należały do użytkownika **Ben**. Korzystając z kluczy, zidentyfikowaliśmy innych użytkowników na koncie i uzyskaliśmy dostęp do poufnych informacji przechowywanych w zasobnikach S3. Wrażliwy plik został pomyślnie pobrany do dalszej inspekcji. Natychmiastowe kroki w celu zabezpieczenia środowiska obejmują wyłączenie i rotację naruszonych kluczy, audyt dostępu innych użytkowników oraz zapewnienie mechanizmów monitorowania i ostrzegania w celu wykrywania nieautoryzowanych działań w przyszłości.