EncryptEdge Labs

Cybersecurity Analyst Internship

Task Report

atalmamun@gmail.com

Task No: 20

Credit: Offensive Security

Table of Contents

1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

Cloud computing has transformed the way organizations store, manage, and access their data and applications. However, with this shift comes a new set of security challenges, especially in widely adopted platforms like Amazon Web Services (AWS). Cloud security involves a set of policies, controls, and technologies designed to protect cloud-based systems, data, and infrastructure. This task explores the core concepts of cloud security, with a focus on AWS, highlighting the shared responsibility model, security risks, and the tools AWS provides to help mitigate those risks.

1.2 Objective

The primary objective of this task is to develop a foundational understanding of cloud security in AWS environments. This includes:

- Understanding the unique security challenges associated with cloud infrastructure.
- Learning the shared responsibility model and the division of security tasks between AWS and its customers.
- Gaining hands-on experience with AWS security tools such as IAM, CloudTrail, and GuardDuty.
- Practicing secure configurations using the AWS Management Console and AWS CLI.

1.3 Requirements

To successfully complete this task, the following tools and components were required:

- Access to a sample AWS environment, including:
    - IAM users and roles
    - EC2 instances
    - S3 buckets
- AWS Management Console for GUI-based interaction with AWS services.
- AWS Command Line Interface (CLI) for command-based AWS operations.
- Access to the following hands-on labs:
    - *Cybr Lab: Getting Started with the AWS CLI*
    - *Cybr Lab: Introduction to AWS IAM Enumeration*
    - *(Optional) TryHackMe Lab: Intro to Cloud Security*
- Ability to capture screenshots of lab activities and configurations.

2.0 Cloud Security Concepts and Challenges

Cloud environments offer flexibility, scalability, and cost-efficiency, but they also introduce distinct security considerations. As organizations increasingly rely on cloud platforms such as Amazon Web Services (AWS), understanding the security framework and tools provided by the platform becomes essential. This section covers the key concepts of cloud security, focusing on AWS's **shared responsibility model**, **common cloud security risks**, and **AWS-native solutions** for mitigating these risks.

2.1 The Shared Responsibility Model

The shared responsibility model is a core principle of cloud security, outlining the division of security responsibilities between AWS and its customers.

- **AWS's Responsibility – "Security of the Cloud":**
  AWS is responsible for securing the underlying infrastructure that runs all the

services offered in the AWS Cloud. This includes:

- Physical security of data centers
- Hardware, software, and networking infrastructure
- Facilities that support cloud services

- **Customer's Responsibility – "Security in the Cloud":**
  Customers are responsible for securing everything that they deploy within AWS. This includes:

  - Management of IAM users, groups, roles, and policies
  - Configuration of security groups and network access control lists
  - Data encryption (at rest and in transit)
  - OS-level security, patching, and firewall configurations for EC2 instances
  - Ensuring application-level security

This model empowers customers with flexibility while emphasizing the need for proper configurations and security practices on their part.

2.2 AWS Cloud Security Risks and Mitigation Tools

Securing cloud resources requires awareness of potential vulnerabilities and a proactive approach to threat mitigation. Below are common security risks and the AWS-native tools used to address them:

2.2.1 Common Security Risks in AWS

- **Misconfigured Access Controls:** Open S3 buckets, overly permissive IAM roles, and misconfigured security groups.

- **Insufficient Identity Management:** Weak IAM policies or lack of multi-factor authentication.

- **Insecure APIs and Interfaces:** Poorly secured endpoints vulnerable to exploitation.

- **Lack of Monitoring and Logging:** Inadequate tracking of user and resource activity.

- **Data Breaches and Loss:** From insider threats or accidental exposure.

2.2.2 AWS Security Tools

- **IAM (Identity and Access Management):**
  Enables the creation and management of users and roles with fine-grained permissions to enforce least privilege access.

- **AWS CloudTrail:**
  Provides detailed event logs of all account activity, enabling auditing and alerting on suspicious behavior.

- **AWS Config:**
  Assesses, audits, and evaluates configurations of AWS resources to ensure compliance with best practices.

- **Amazon GuardDuty:**
  A threat detection service that uses machine learning and AWS data sources to identify unusual or unauthorized activity.

- **AWS Security Hub:**
  Aggregates security alerts and findings from multiple AWS services and partner tools into a single dashboard.

Together, these tools form a comprehensive security ecosystem that helps identify vulnerabilities, enforce policy compliance, and respond to threats effectively.

3.0 Hands-On Lab Completion and Reflections

To reinforce theoretical understanding with practical experience, I completed a series of hands-on labs focusing on AWS CLI operations and IAM enumeration. These exercises provided insight into how cloud security is implemented and managed in real-world scenarios. Below are my reflections on each lab along with key takeaways.

3.1 Cybr Lab: Getting Started with the AWS CLI

Overview:
In this lab, I learned how to configure and use the AWS Command Line Interface (CLI) to interact with AWS services. The CLI is a powerful tool that allows users to automate tasks, manage resources, and retrieve data efficiently from the command line.

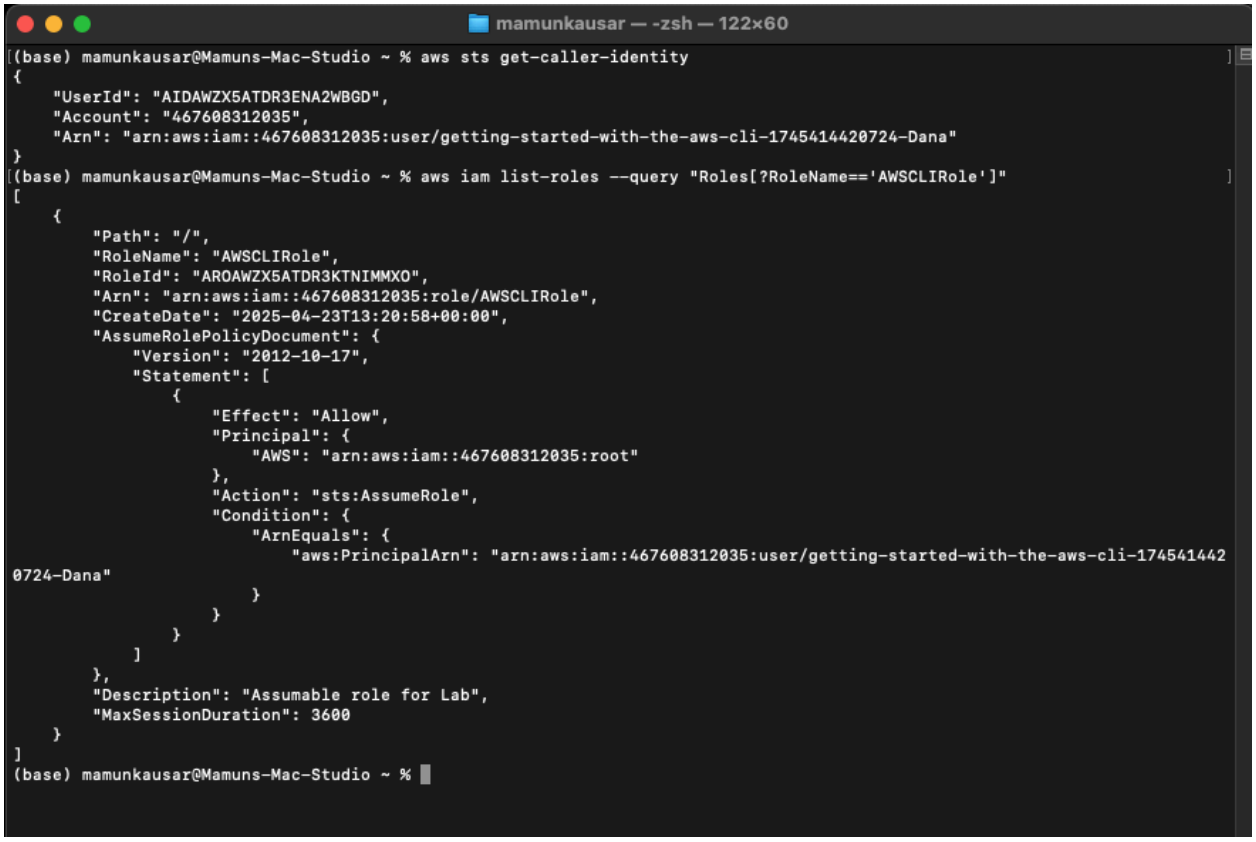
Tasks Performed:

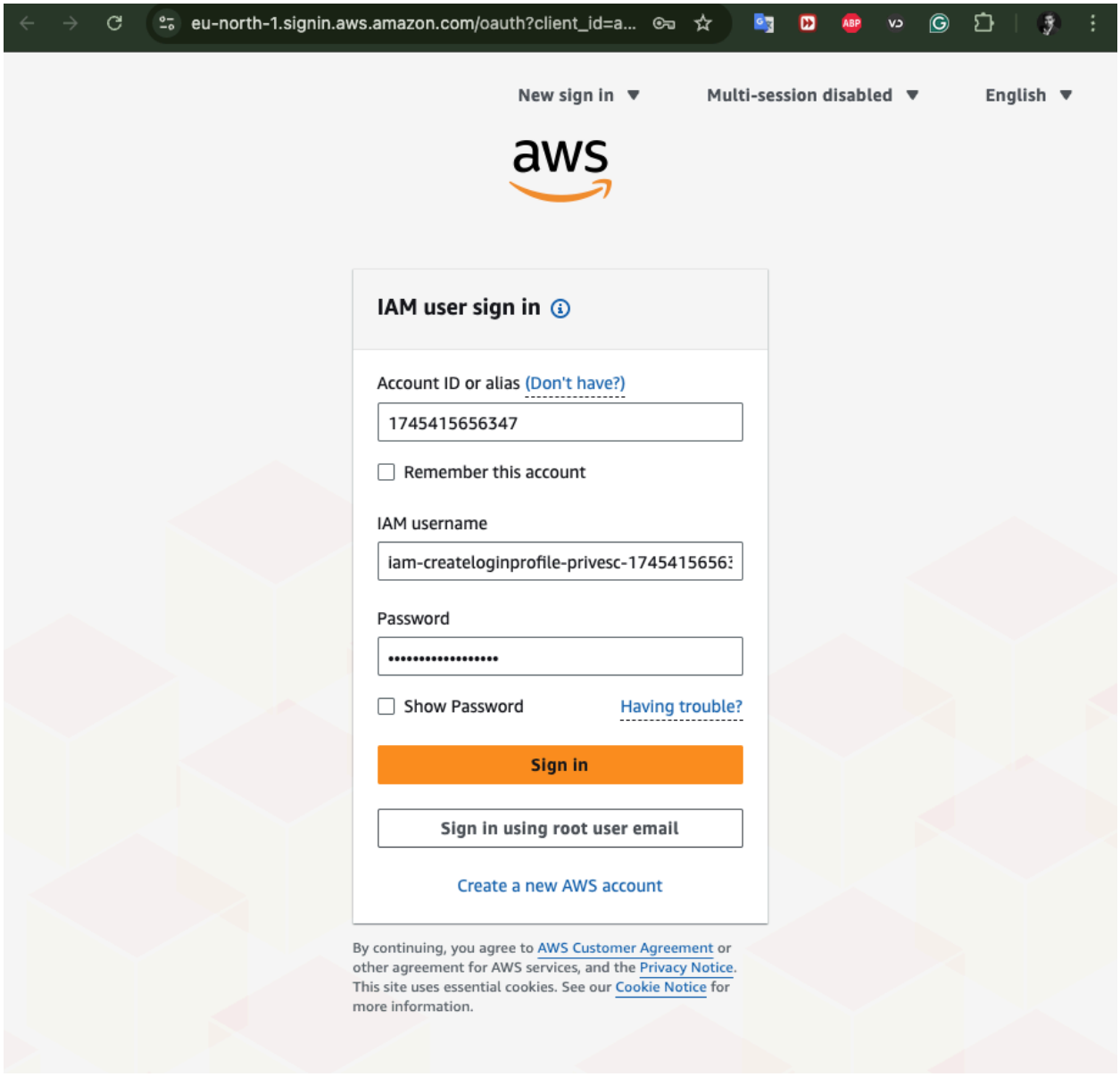
- Installed and configured AWS CLI with access keys.
- Executed commands to list S3 buckets, describe EC2 instances, and retrieve IAM user details.
- Created and managed AWS resources using CLI commands.

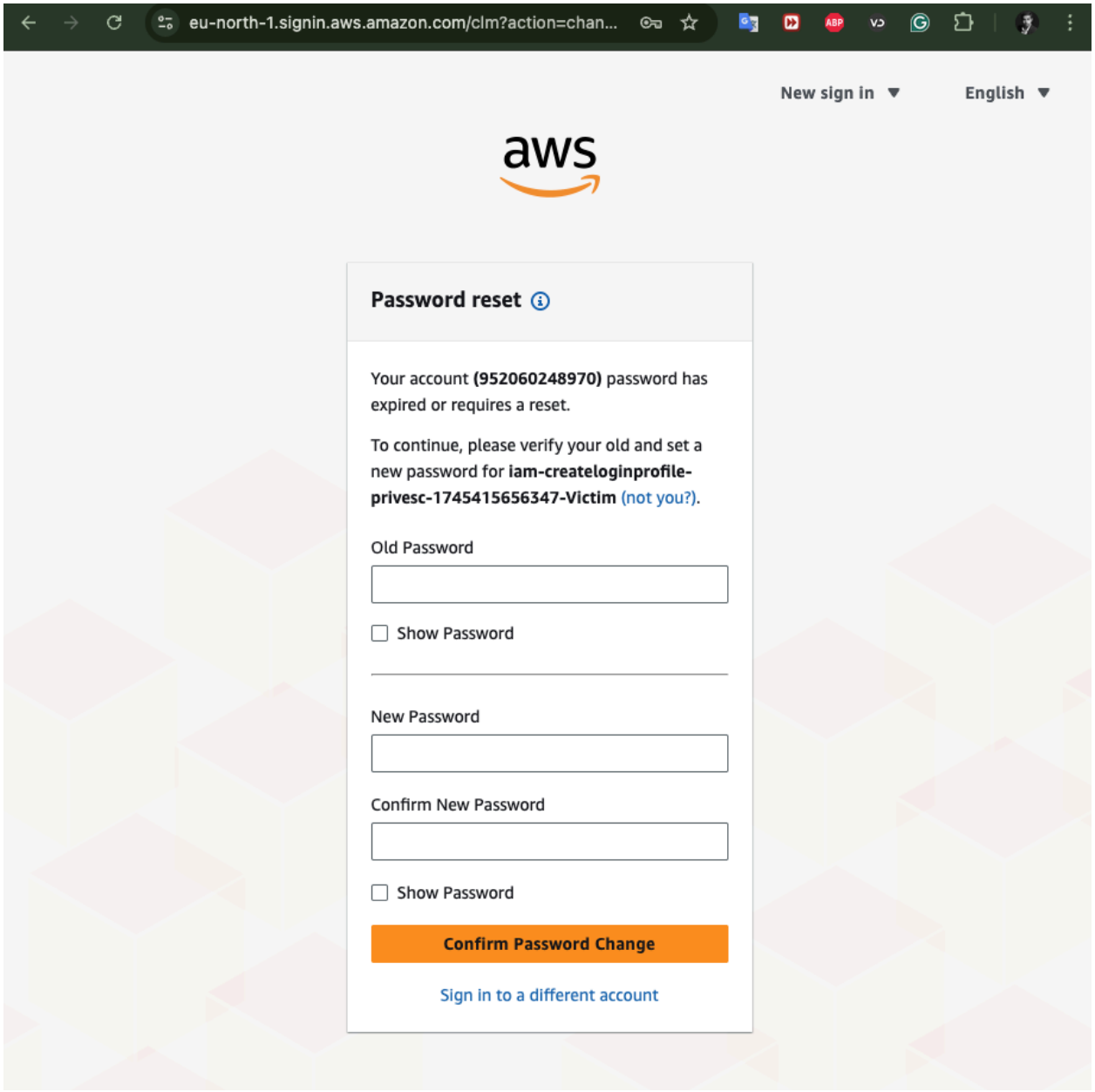
Key Takeaways:

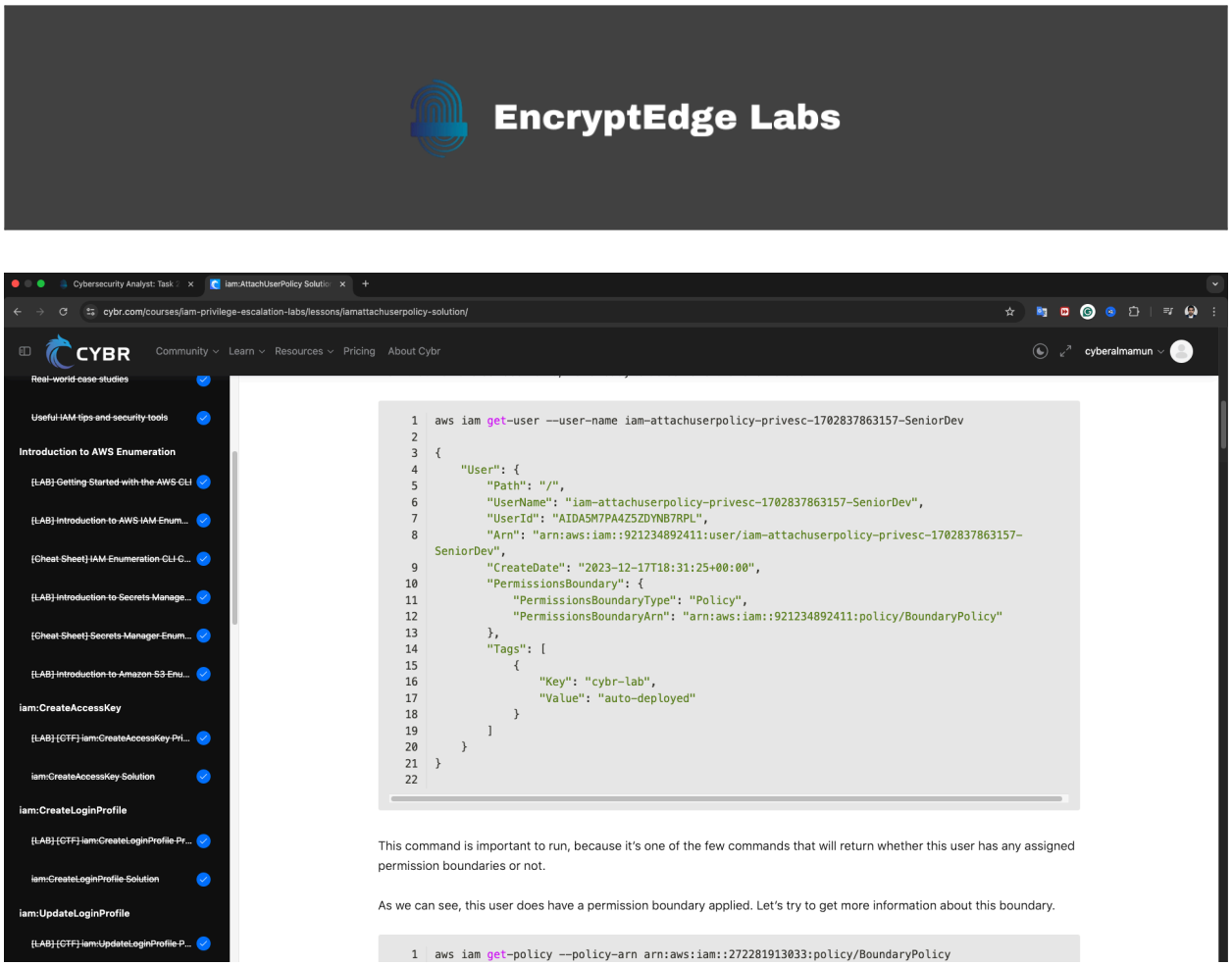
- The AWS CLI significantly enhances efficiency, especially for repetitive tasks or scripting operations.
- Proper configuration of credentials and regions is essential for secure and successful interaction with AWS resources.
- CLI operations require an understanding of IAM permissions—only users with appropriate privileges can perform specific actions.

Screenshots:




eu-north-1.signin.aws.amazon.com/oauth?client_id=a...
New sign in
Multi-session disabled
English
aws
IAM user sign in
Account ID or alias (Don't have?)
1745415656347
Remember this account
IAM username
iam-createloginprofile-privesc-1745415656
Password
Show Password
Having trouble?
Sign in
Sign in using root user email
Create a new AWS account
By continuing, you agree to AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.


eu-north-1.signin.aws.amazon.com/clm?action=chan...
New sign in
English
aws
Password reset
Your account (952060248970) password has expired or requires a reset.
To continue, please verify your old and set a new password for iam-createloginprofile-privesc-1745415656347-Victim (not you?).
Old Password
Show Password
New Password
Confirm New Password
Show Password
Confirm Password Change
Sign in to a different account



3.2 Cybr Lab: Introduction to AWS IAM Enumeration

Overview:

This lab focused on IAM enumeration techniques, an essential process for identifying users, roles, and policies within an AWS environment. Enumeration helps detect potential security misconfigurations and excessive permissions.

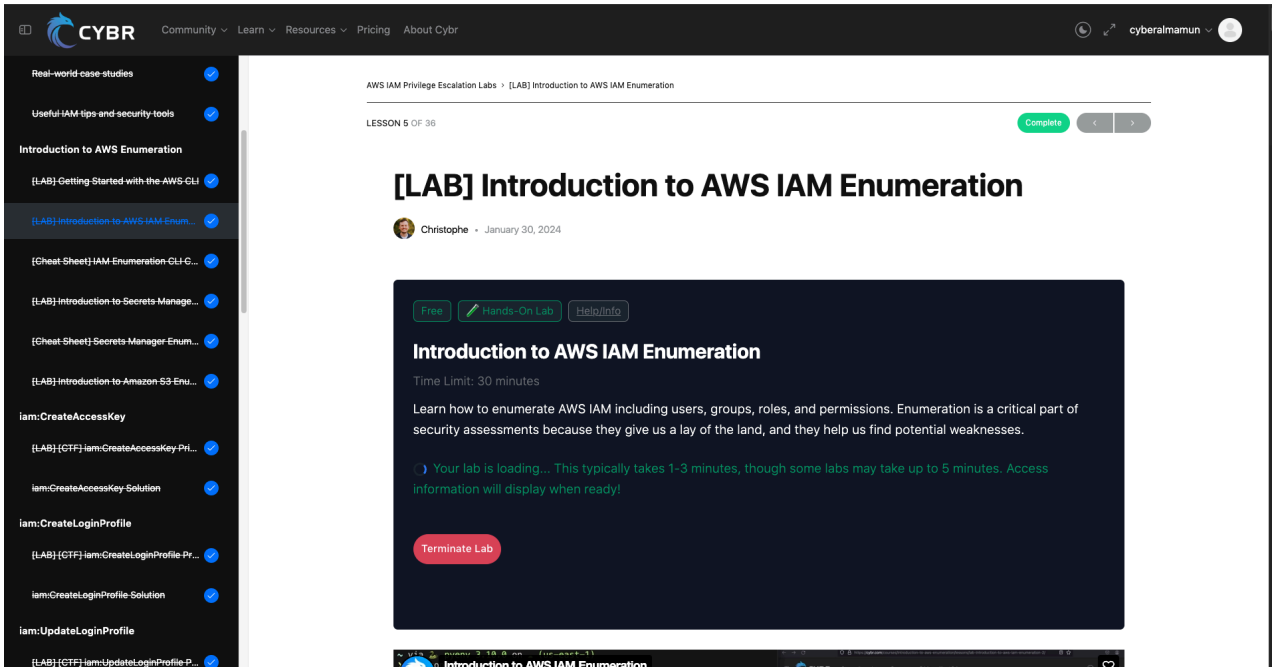
Tasks Performed:

- Enumerated IAM users, roles, and attached policies.
- Analyzed permissions to identify overprivileged accounts.
- Investigated potential vectors for privilege escalation.

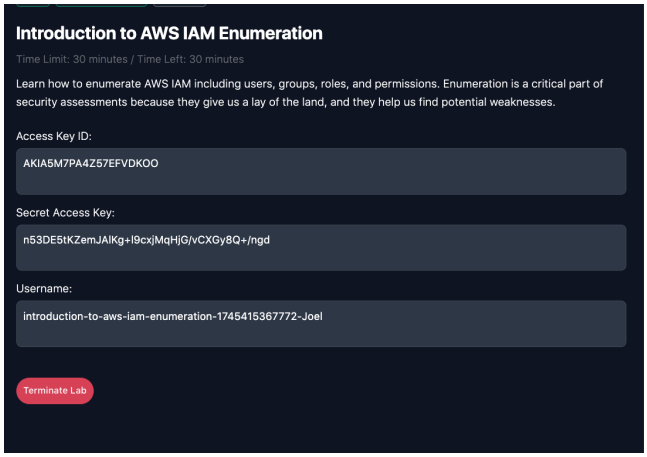
Key Takeaways:

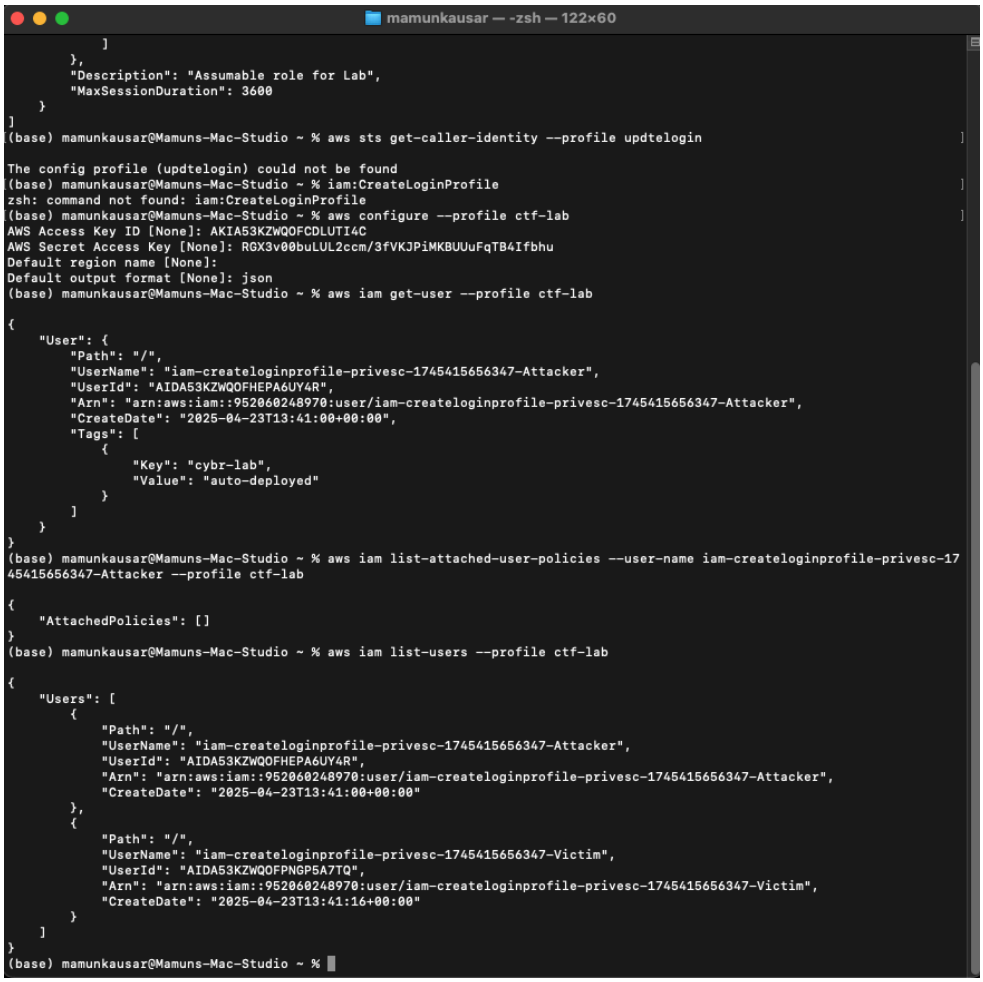
- IAM enumeration is a crucial part of security auditing in AWS. It helps to detect risks like excessive permissions or unused accounts.
- Least privilege principles must be enforced to minimize the attack surface.
- Regular audits of IAM policies are necessary to maintain a secure cloud environment.

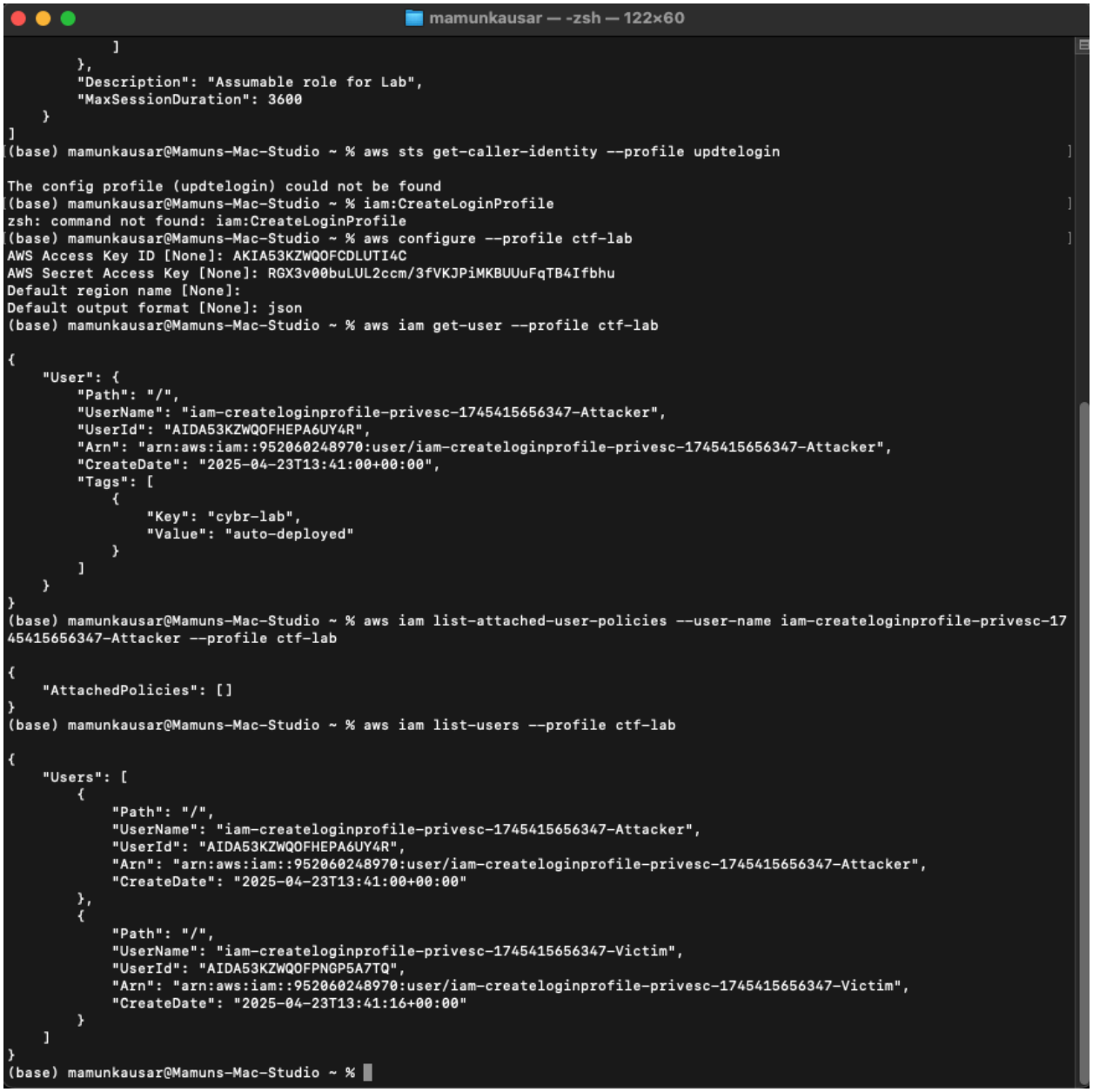
Screenshots:

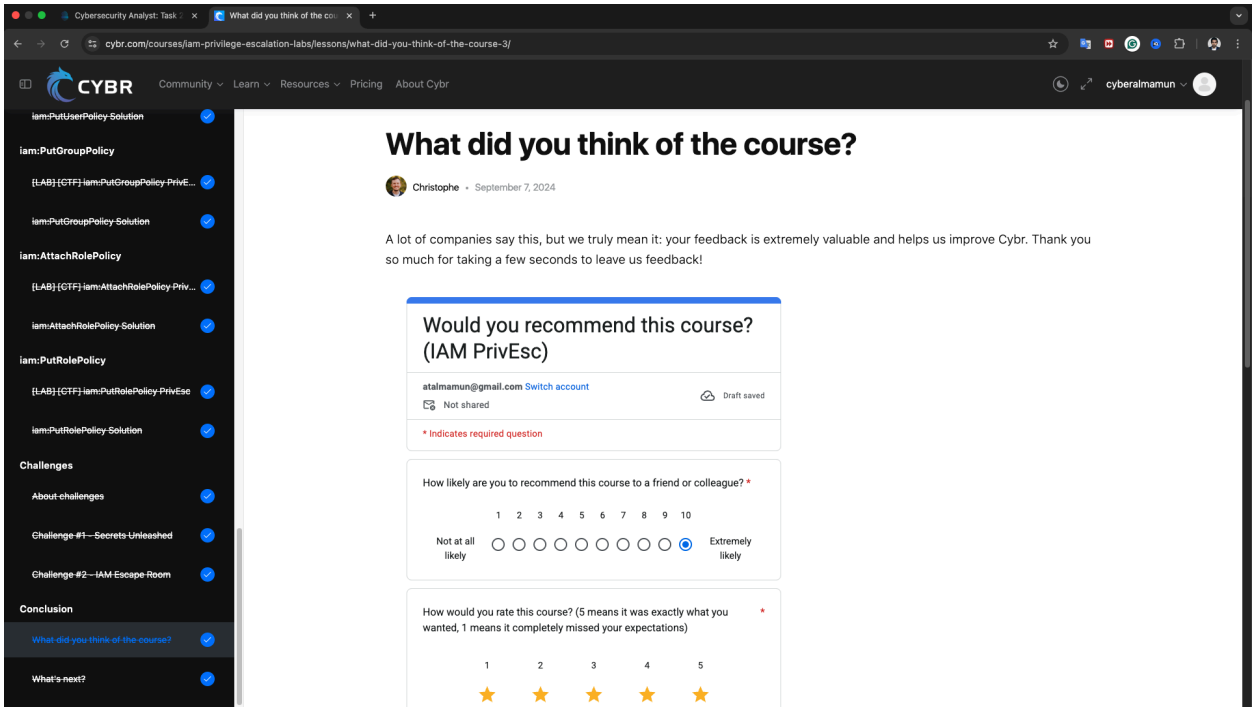


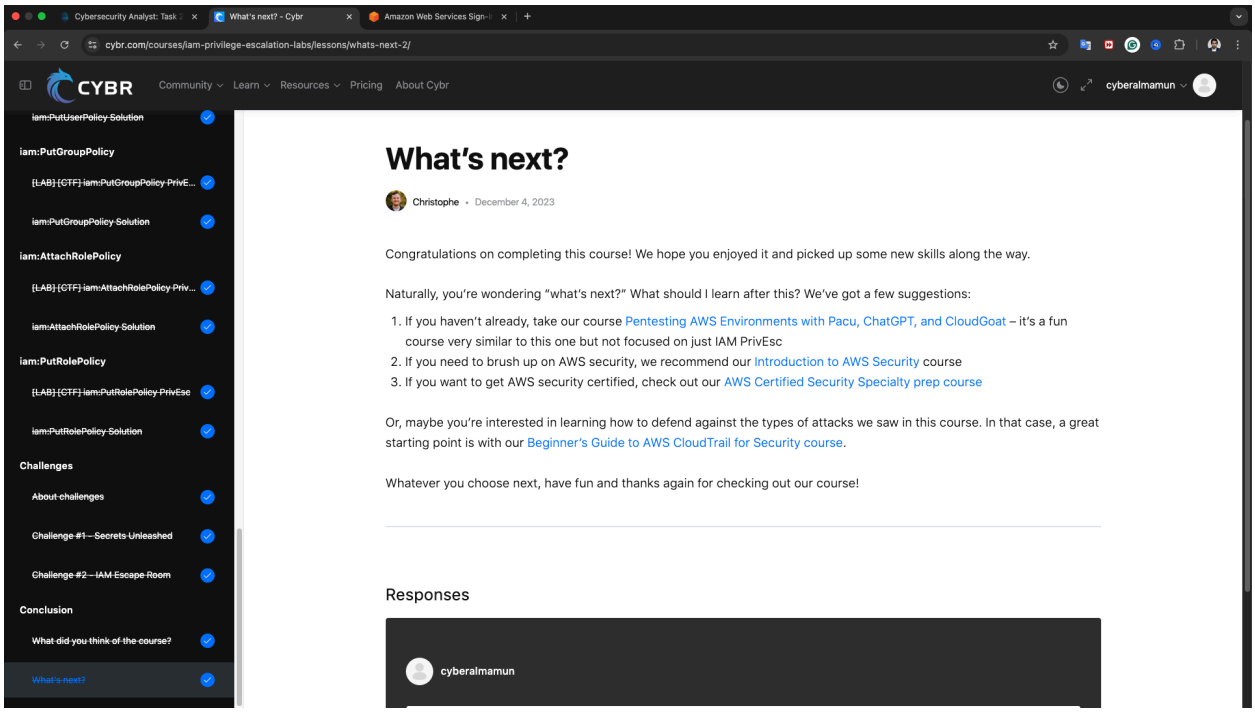

EncryptEdge Labs


Introduction to AWS IAM Enumeration
Time Limit: 30 minutes / Time Left: 30 minutes
Learn how to enumerate AWS IAM including users, groups, roles, and permissions. Enumeration is a critical part of security assessments because they give us a lay of the land, and they help us find potential weaknesses.
Access Key ID:
AKIA5M7PA4Z57EFVDKOO
Secret Access Key:
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
Username:
introduction-to-aws-iam-enumeration-1745415367772-Joel
Terminate Lab


mamunkausar — -zsh — 122×60
]
},
"Description": "Assumable role for Lab",
"MaxSessionDuration": 3600
}
]
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws sts get-caller-identity --profile updtelogin
The config profile (updtelogin) could not be found
(base) mamunkausar@Mamuns-Mac-Studio ~ % iam:CreateLoginProfile
zsh: command not found: iam:CreateLoginProfile
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws configure --profile ctf-lab
AWS Access Key ID [None]: AKIA53KZWQOFCDLUTI4C
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]: json
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws iam get-user --profile ctf-lab
{
"User": {
"Path": "/",
"UserName": "iam-createloginprofile-privesc-1745415656347-Attacker",
"UserId": "AIDA53KZWQOFHEPA6UY4R",
"Arn": "arn:aws:iam::952060248970:user/iam-createloginprofile-privesc-1745415656347-Attacker",
"CreateDate": "2025-04-23T13:41:00+00:00",
"Tags": [
{
"Key": "cybr-lab",
"Value": "auto-deployed"
}
]
}
}
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws iam list-attached-user-policies --user-name iam-createloginprofile-privesc-1745415656347-Attacker --profile ctf-lab
{
"AttachedPolicies": []
}
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws iam list-users --profile ctf-lab
{
"Users": [
{
"Path": "/",
"UserName": "iam-createloginprofile-privesc-1745415656347-Attacker",
"UserId": "AIDA53KZWQOFHEPA6UY4R",
"Arn": "arn:aws:iam::952060248970:user/iam-createloginprofile-privesc-1745415656347-Attacker",
"CreateDate": "2025-04-23T13:41:00+00:00"
},
{
"Path": "/",
"UserName": "iam-createloginprofile-privesc-1745415656347-Victim",
"UserId": "AIDA53KZWQOFPNGP5A7TQ",
"Arn": "arn:aws:iam::952060248970:user/iam-createloginprofile-privesc-1745415656347-Victim",
"CreateDate": "2025-04-23T13:41:16+00:00"
}
]
}
(base) mamunkausar@Mamuns-Mac-Studio ~ %


mamunkausar — -zsh — 122×60
]
},
"Description": "Assumable role for Lab",
"MaxSessionDuration": 3600
}
]
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws sts get-caller-identity --profile updtelogin
The config profile (updtelogin) could not be found
(base) mamunkausar@Mamuns-Mac-Studio ~ % iam:CreateLoginProfile
zsh: command not found: iam:CreateLoginProfile
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws configure --profile ctf-lab
AWS Access Key ID [None]: AKIA53KZWQOFCDLUTI4C
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]: json
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws iam get-user --profile ctf-lab
{
"User": {
"Path": "/",
"UserName": "iam-createloginprofile-privesc-1745415656347-Attacker",
"UserId": "AIDA53KZWQOFHEPA6UY4R",
"Arn": "arn:aws:iam::952060248970:user/iam-createloginprofile-privesc-1745415656347-Attacker",
"CreateDate": "2025-04-23T13:41:00+00:00",
"Tags": [
{
"Key": "cybr-lab",
"Value": "auto-deployed"
}
]
}
}
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws iam list-attached-user-policies --user-name iam-createloginprofile-privesc-17
45415656347-Attacker --profile ctf-lab
{
"AttachedPolicies": []
}
(base) mamunkausar@Mamuns-Mac-Studio ~ % aws iam list-users --profile ctf-lab
{
"Users": [
{
"Path": "/",
"UserName": "iam-createloginprofile-privesc-1745415656347-Attacker",
"UserId": "AIDA53KZWQOFHEPA6UY4R",
"Arn": "arn:aws:iam::952060248970:user/iam-createloginprofile-privesc-1745415656347-Attacker",
"CreateDate": "2025-04-23T13:41:00+00:00"
},
{
"Path": "/",
"UserName": "iam-createloginprofile-privesc-1745415656347-Victim",
"UserId": "AIDA53KZWQOFPNGP5A7TQ",
"Arn": "arn:aws:iam::952060248970:user/iam-createloginprofile-privesc-1745415656347-Victim",
"CreateDate": "2025-04-23T13:41:16+00:00"
}
]
}
(base) mamunkausar@Mamuns-Mac-Studio ~ %


cybr.com/courses/iam-privilege-escalation-labs/lessons/what-did-you-think-of-the-course-3/
CYBR
Community
Learn
Resources
Pricing
About Cybr
cyberalmamun
iam:PutUserPolicy Solution
iam:PutGroupPolicy
[LAB] [CTF] iam:PutGroupPolicy PrivE...
iam:PutGroupPolicy Solution
iam:AttachRolePolicy
[LAB] [CTF] iam:AttachRolePolicy Priv...
iam:AttachRolePolicy Solution
iam:PutRolePolicy
[LAB] [CTF] iam:PutRolePolicy PrivEsc
iam:PutRolePolicy Solution
Challenges
About challenges
Challenge #1 – Secrets Unleashed
Challenge #2 – IAM Escape Room
Conclusion
What did you think of the course?
What's next?
What did you think of the course?
Christophe • September 7, 2024
A lot of companies say this, but we truly mean it: your feedback is extremely valuable and helps us improve Cybr. Thank you so much for taking a few seconds to leave us feedback!
Would you recommend this course? (IAM PrivEsc)
ataImamun@gmail.com Switch account
Not shared
Draft saved
* Indicates required question
How likely are you to recommend this course to a friend or colleague? *
1 2 3 4 5 6 7 8 9 10
Not at all likely
Extremely likely
How would you rate this course? (5 means it was exactly what you wanted, 1 means it completely missed your expectations) *
1 2 3 4 5


cybr.com/courses/iam-privilege-escalation-labs/lessons/whats-next-2/
What's next? - Cybr
Amazon Web Services Sign-I
CYBR
Community
Learn
Resources
Pricing
About Cybr
cyberalmamun
iam:PutUserPolicy Solution
iam:PutGroupPolicy
[LAB] [CTF] iam:PutGroupPolicy PrivE...
iam:PutGroupPolicy Solution
iam:AttachRolePolicy
[LAB] [CTF] iam:AttachRolePolicy Priv...
iam:AttachRolePolicy Solution
iam:PutRolePolicy
[LAB] [CTF] iam:PutRolePolicy PrivEsc
iam:PutRolePolicy Solution
Challenges
About challenges
Challenge #1 – Secrets Unleashed
Challenge #2 – IAM Escape Room
Conclusion
What did you think of the course?
What's next?
What's next?
Christophe • December 4, 2023
Congratulations on completing this course! We hope you enjoyed it and picked up some new skills along the way.
Naturally, you're wondering "what's next?" What should I learn after this? We've got a few suggestions:
1. If you haven't already, take our course Pentesting AWS Environments with Pacu, ChatGPT, and CloudGoat – it's a fun course very similar to this one but not focused on just IAM PrivEsc
2. If you need to brush up on AWS security, we recommend our Introduction to AWS Security course
3. If you want to get AWS security certified, check out our AWS Certified Security Specialty prep course
Or, maybe you're interested in learning how to defend against the types of attacks we saw in this course. In that case, a great starting point is with our Beginner's Guide to AWS CloudTrail for Security course.
Whatever you choose next, have fun and thanks again for checking out our course!
Responses
cyberalmamun

3.3 Optional Lab: TryHackMe – Intro to Cloud Security

Overview:
This optional lab provided an introduction to broader cloud security principles. It emphasized best practices for cloud infrastructure security and introduced tools used to monitor, detect, and respond to threats in cloud environments.

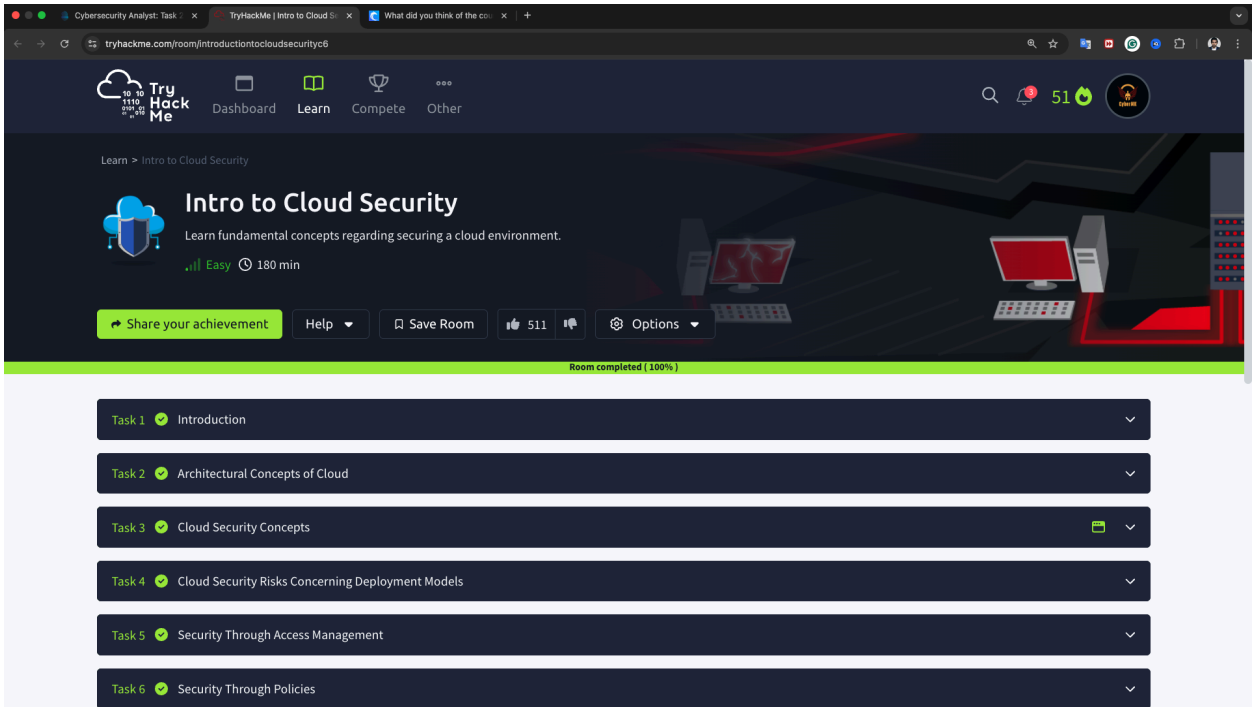
Tasks Performed:

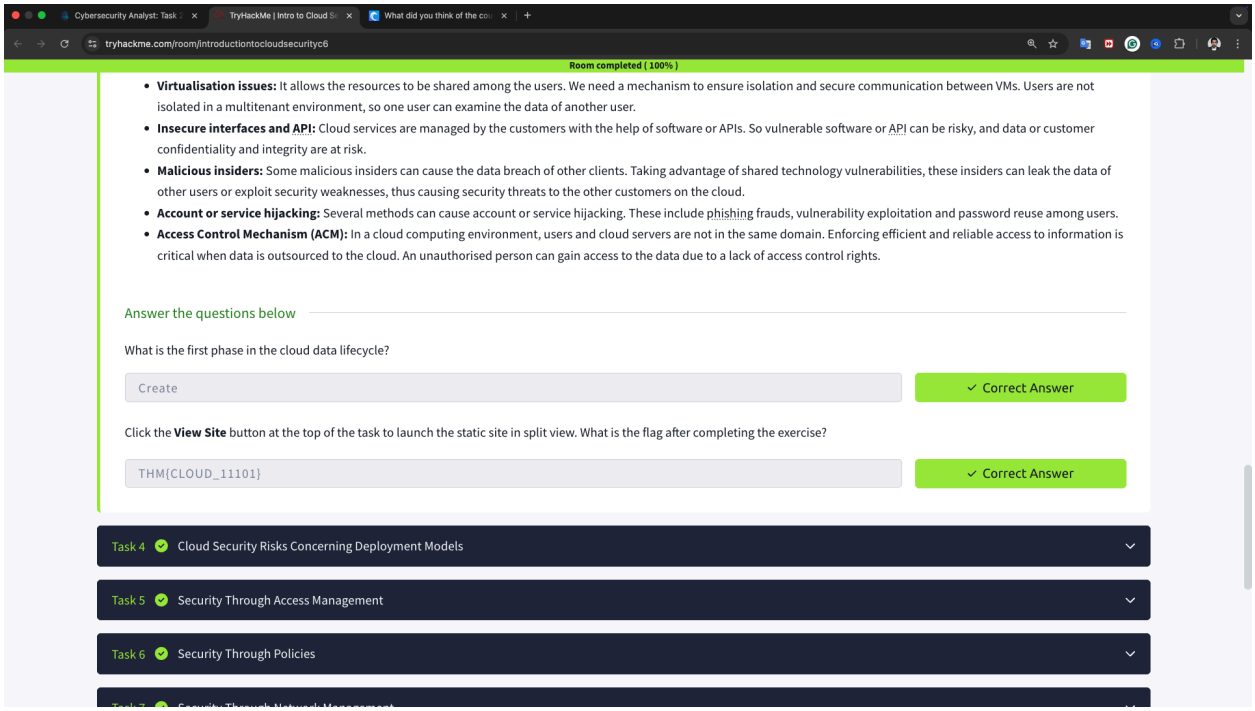
- Explored common attack vectors in cloud setups.
- Used basic threat detection tools in simulated environments.
- Learned about encryption, monitoring, and access control techniques.

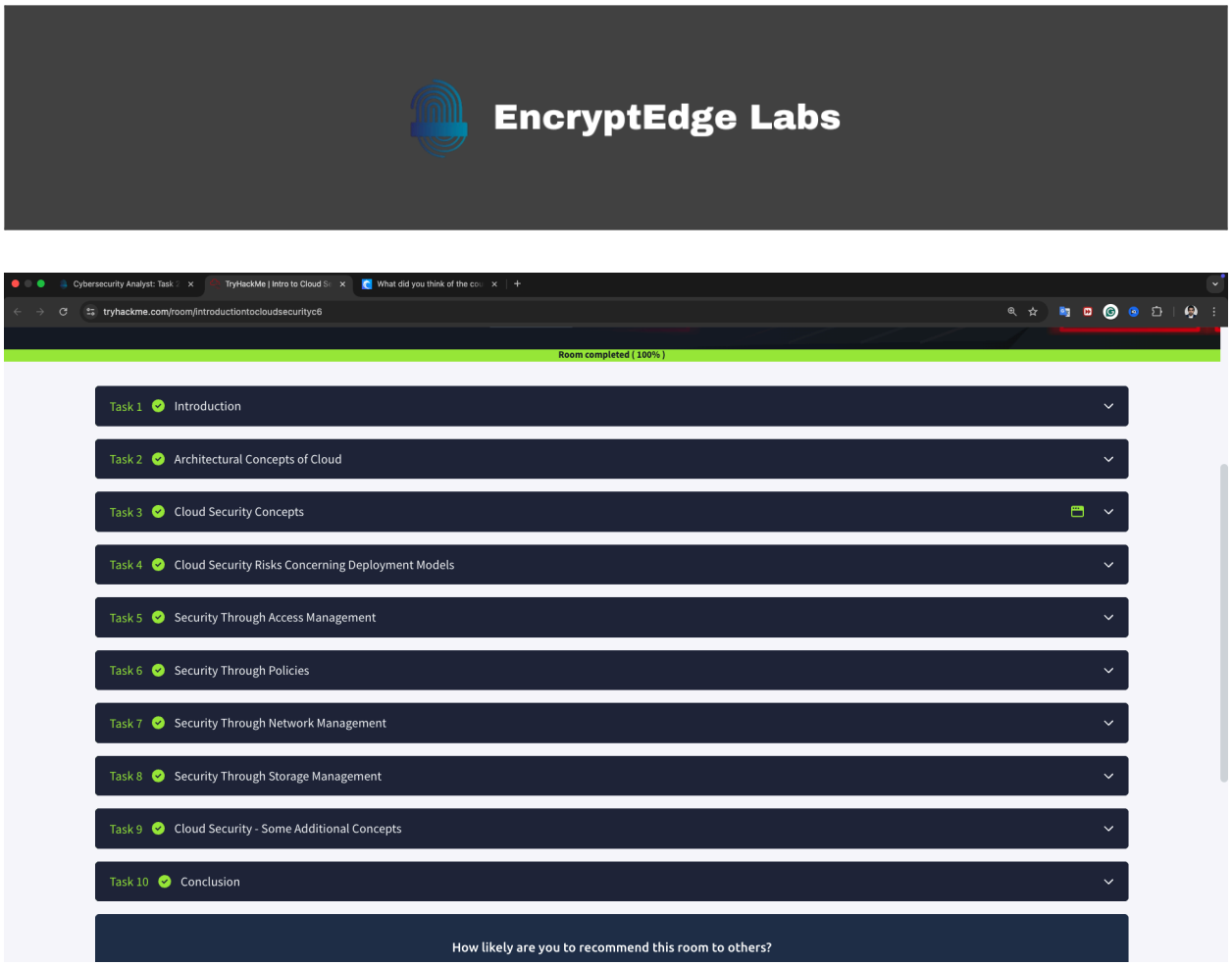
Key Takeaways:

- Cloud environments must be actively monitored using both native and third-party tools.
- Threat modeling and risk assessment are critical for identifying gaps in security posture.
- This lab emphasized the importance of a layered defense strategy in cloud security.

Screenshots:


tryhackme.com/room/introductiontocloudsecurityc6
Try Hack Me
Dashboard
Learn
Compete
Other
51
Learn > Intro to Cloud Security
Intro to Cloud Security
Learn fundamental concepts regarding securing a cloud environment.
Easy
180 min
Share your achievement
Help
Save Room
511
Options
Room completed (100%)
Task 1 Introduction
Task 2 Architectural Concepts of Cloud
Task 3 Cloud Security Concepts
Task 4 Cloud Security Risks Concerning Deployment Models
Task 5 Security Through Access Management
Task 6 Security Through Policies


tryhackme.com/room/introductiontocloudsecurityc6
Room completed (100%)
Virtualisation issues: It allows the resources to be shared among the users. We need a mechanism to ensure isolation and secure communication between VMs. Users are not isolated in a multitenant environment, so one user can examine the data of another user.
Insecure interfaces and API: Cloud services are managed by the customers with the help of software or APIs. So vulnerable software or API can be risky, and data or customer confidentiality and integrity are at risk.
Malicious insiders: Some malicious insiders can cause the data breach of other clients. Taking advantage of shared technology vulnerabilities, these insiders can leak the data of other users or exploit security weaknesses, thus causing security threats to the other customers on the cloud.
Account or service hijacking: Several methods can cause account or service hijacking. These include phishing frauds, vulnerability exploitation and password reuse among users.
Access Control Mechanism (ACM): In a cloud computing environment, users and cloud servers are not in the same domain. Enforcing efficient and reliable access to information is critical when data is outsourced to the cloud. An unauthorised person can gain access to the data due to a lack of access control rights.
Answer the questions below
What is the first phase in the cloud data lifecycle?
Create
Correct Answer
Click the View Site button at the top of the task to launch the static site in split view. What is the flag after completing the exercise?
THM{CLOUD_11101}
Correct Answer
Task 4 Cloud Security Risks Concerning Deployment Models
Task 5 Security Through Access Management
Task 6 Security Through Policies



4.0 Conclusion

The completion of Task 20: *Cloud Security Basics* provided a valuable introduction to securing cloud environments, particularly within Amazon Web Services (AWS). Through both theoretical exploration and hands-on practice, I gained a deeper understanding of how to approach cloud security challenges effectively.

The **shared responsibility model** was a key concept, clarifying the distinct roles of AWS and its customers in maintaining security. This model emphasized the need for organizations to take ownership of securing the elements they deploy within the cloud, such as IAM configurations, data protection, and resource permissions.

By engaging in practical labs, I developed foundational skills in using the **AWS CLI**, performing **IAM enumeration**, and identifying potential misconfigurations. These experiences underscored the importance of:

- Enforcing the **principle of least privilege**
- Regularly auditing IAM roles and policies
- Leveraging AWS-native tools like **CloudTrail**, **GuardDuty**, and **Security Hub** to maintain visibility and respond to threats

Overall, this task enhanced my confidence in working with AWS security tools and provided a clear roadmap for further learning in cloud security. As cloud adoption continues to rise, understanding and applying these security fundamentals is crucial for any cybersecurity professional.

EncryptEdge Labs

This Internship Task report was developed on [April, 23, 2025]

By:

atalmamun@gmail.com