



OFFENSIVE CLOUD SECURITY TRAINING

Exam Report

OASP • OAWSP • OASE



CloudBreach ID	cbxxxx
Candidate Name	
Email Address	
Certification	OASP / OAWSP / OASE (Select one)

Exam Date	XX / XX / XX
Report Version	1.0



Reporting Requirements

Read this section before you begin.

This document is the sole basis on which your exam is graded. Screenshots and prose in this report must prove that you completed each objective yourself. Follow these requirements:

- Document every exam objective you completed. If a step is not in the report, it did not happen for grading purposes.
- Every screenshot must be legible and, where required, show your CloudBreach ID or the required control string in-frame.
- Include the exact commands you ran in the code blocks so a grader can follow and reproduce your chain.
- Record proof strings / flags in the Proof Collection table as you capture them, and screenshot each one in its step.
- Do not fabricate or embellish results. Partial, honest work scores; invented work does not.
- Export to PDF before submitting unless the exam instructions state otherwise. Confirm all images render in the exported file.

Item	Requirement
File name	cb<ID>_<certification>_exam_report.pdf
Format	PDF
Max file size	Per exam instructions
Submission	Per exam instructions

Table of Contents

Reporting Requirements.....	1
Table of Contents.....	1
Executive Summary.....	1
Objective.....	1
Approach & Outcome.....	1
Results at a Glance.....	1
Attack Path Overview.....	1
Compromise Chain.....	1
Diagram.....	1
Walkthrough.....	1
Step 1 — <short title of this step>.....	1
Step 2 — <short title of this step>.....	1
Proof Collection.....	1
Cleanup & Housekeeping.....	1
Recommendations.....	1
Conclusion.....	1



Executive Summary

This report documents the activities completed during the CloudBreach Offensive Cloud Security certification exam. It is evaluated on accuracy, completeness, and coverage of the exam objectives, and demonstrates the technical skills required for the certification.

Objective

State the goal of the exam in one or two sentences (e.g. gain access to the target Azure/AWS environment and demonstrate control of the required resources / capture all proof strings).

Approach & Outcome

Summarise your overall approach and result in 3–5 sentences: how you gained initial access, how you escalated, and which objectives you achieved. Keep it high level; the detail lives in the Walkthrough.

Results at a Glance

Objective / Target	Status	Proof captured

Status: Completed / Partial / Not attempted.

Attack Path Overview

Outline the full compromise chain from initial access to the final objective. A diagram is ideal; a numbered list of the key hops is the minimum.

Compromise Chain

- Initial access: <how you first got a foothold>
- Enumeration: <what you discovered>
- Privilege escalation / lateral movement: <how you expanded access>
- Objective reached: <what proved success>

Diagram (Optional)

[Insert diagram to show the full compromise chain]

Walkthrough

Document each step of your attack chain in order. Copy the Step block below for as many steps as you need, and give each a short descriptive title.

Step 1 - <short title of this step>

OBJECTIVE

What this step is trying to achieve and why it moves you toward the exam objective.

TARGET / SCOPE

Host, IP, URL, tenant, subscription or resource this step touches.

VULNERABILITY / TECHNIQUE

Name the weakness and map it to MITRE ATT&CK where relevant (e.g. T1078 Valid Accounts).

TOOLS & COMMANDS

The exact commands you ran, copy-paste-able, so a grader can reproduce them.

```
$ <paste the exact command(s) you ran here>
```

FINDINGS

What the output told you and how you used it in the next step.

EVIDENCE

Screenshot showing the result. Must be legible and show your CloudBreach ID / control string where possible.

[Insert screenshot as proof - include the terminal, target host/IP, and result in-frame]

Step 2 - <short title of this step>

OBJECTIVE

What this step is trying to achieve and why it moves you toward the exam objective.

TARGET / SCOPE

Host, IP, URL, tenant, subscription or resource this step touches.

VULNERABILITY / TECHNIQUE

Name the weakness and map it to MITRE ATT&CK where relevant (e.g. T1078 Valid Accounts).

TOOLS & COMMANDS

The exact commands you ran, copy-paste-able, so a grader can reproduce them.

```
$ <paste the exact command(s) you ran here>
```

FINDINGS

What the output told you and how you used it in the next step.

EVIDENCE



Screenshot showing the result. Must be legible and show your CloudBreach ID / control string where required.

[Insert screenshot as proof — include the terminal, target host/IP, and result in-frame]

▲ Copy the Step block above for each additional step ▲



Proof Collection

Record every proof string / flag you captured. Each one must also be shown in a screenshot inside its Walkthrough step.

#	Target / Location	Proof string / flag	Step ref.
1			
2			
3			
4			

Recommendations (Optional)

Optional but encouraged: for each key finding, give a short remediation the defender could apply. Map to the relevant control where possible.

- Finding: <weakness> → Remediation: <fix>

Conclusion

Summarise the objectives achieved, proof strings captured, and your overall result. Keep it to a few sentences.