SECUREU

WE MAKE SECURITY ACCESSIBLE

CLOUD PENETRATION TESTING

SECURITY REPORT

DEMO CORP

DATE : DD MONTH YYYY

VERSION : 1.0

Confidential Document

Attention : This document contains confidential and privileged information for the intended recipient only. Any unauthorized disclosure, copying or distribution is prohibited. By accepting this document, you agree to maintain its confidentiality.

CONTENTS ...

1. Confidentiality Statement

This document is the exclusive property of Demo Corp and SECUREU. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires the consent of both Demo Corp and SECUREU.

Demo Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

2. Disclaimer

This Cloud penetration test was performed by scanning the Cloud owned by Demo Corp for identifying potential security weaknesses and vulnerabilities in Demo Corp's Cloud infrastructure.

A penetration test is considered as a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

3. Contact Information

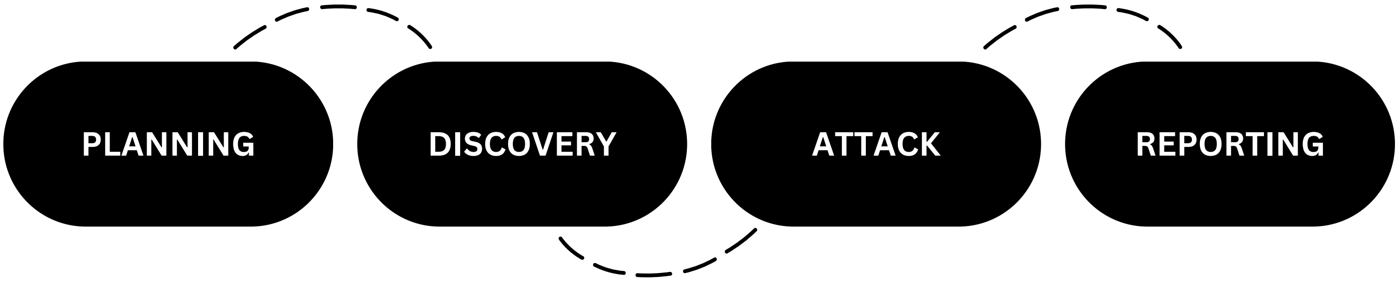
Name	Title	Contact Information
John	Lead Penetration Tester	john@secureu.in
Albert	Security Engineer	albert@secureu.in
Gilbert	Penetration Tester	gilbert@secureu.in

4. Assessment Overview

From <month> xth, 20XX to <month> yth, 20XX SECUREU attempted to evaluate the security posture of the Cloud Infrastructure of Demo Corp and compared it to the current industry best practices by performing a penetration test

Phases of penetration testing activities include the following:

- **Planning** – Customer goals are gathered and rules of engagement obtained.
- **Discovery** – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- **Attack** – Confirm potential vulnerabilities through exploitation and perform additional discoveries upon new access.
- **Reporting** – Document all found vulnerabilities, exploits, failed attempts, and company strengths and weaknesses.



5. Assessment Components

5.1. Cloud Penetration Test

A Cloud penetration test simulates the role of an attacker from outside the network. An engineer will scan the Cloud infrastructure that faces the internet to identify potential vulnerabilities.

6. Finding Severity Ratings

The following table defines levels of severity and the corresponding CVSS score range used throughout the document to assess vulnerability and risk impact.

SEVERITY	CVSS V3 SCORE RANGE	DEFINITIONS
Critical	9.0-10.0	**Exploitation:** • Exploitation is straightforward. • Results in system-level compromise. **Plan of Action:** • Patch immediately.
High	7.0-8.9	**Exploitation**: • Exploitation is more difficult. Could cause elevated privileges. • Potential to cause loss of data or downtime. **Plan of Action**: • Patch as soon as possible.
Medium	4.0-6.9	**Exploitation:** • Vulnerabilities exist but are not exploitable. • Might require extra steps to make the vulnerability exploitable. **Plan of Action**: • Patch after high-priority issues has been resolved.
Low	0.1-3.9	**Exploitation:** • Vulnerabilities are non-exploitable. • Mitigation would reduce an organization’s attack surface. **Plan of Action:** • Patch during the next maintenance window.
Informational	N/A	• No vulnerability exists. • Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

7. Risk Factors

Risk is measured by two factors: Likelihood & Impact

7.1. Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

7.2. Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity and availability of client systems and/or data, reputational harm, and financial loss.

8. Scope

ASSESSMENT	DETAILS
Cloud Vulnerability Scan	democorp.com

8.1. Scope Exclusions

SECUREU did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were covered in penetration testing of the Cloud

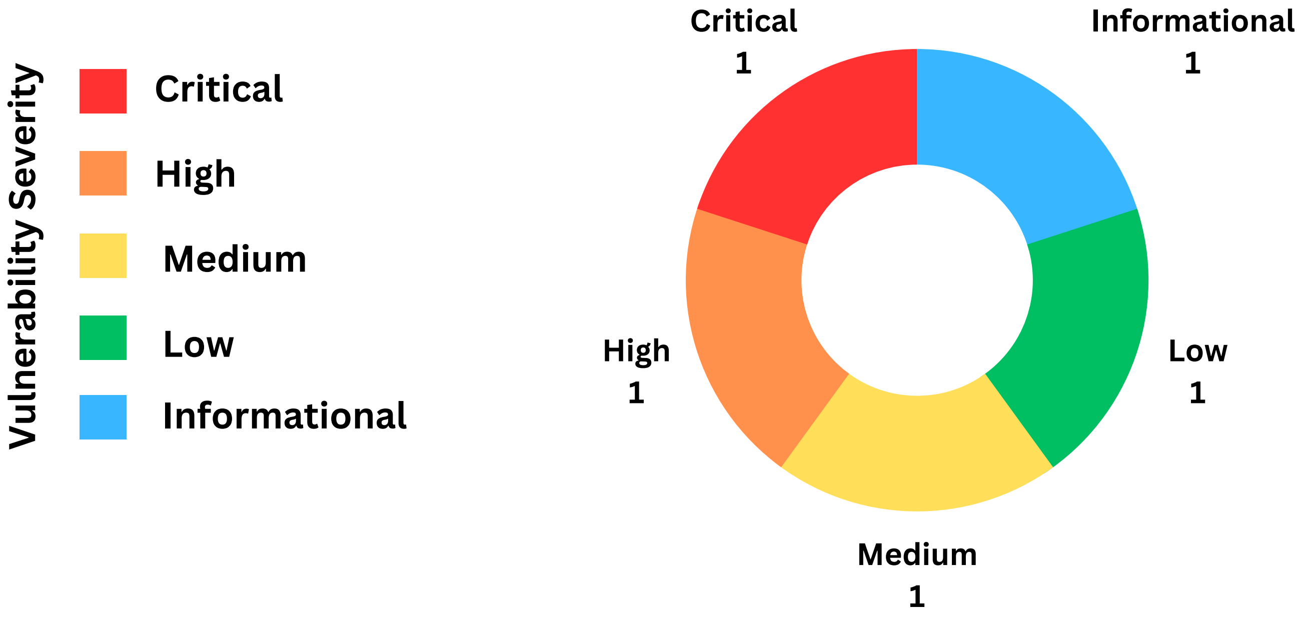
9. Executive Summary

SECUREU evaluated Demo Corp's external security posture through a Cloud penetration test from <month> xth, 20XX to <month> Yth, 20XX. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

B

Security Rating

VULNERABILITY DISTRIBUTION



9.1. Scoping and Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

9.2. Testing Summary

The Cloud assessment evaluated Demo Corp's security posture. The SECUREU team performed vulnerability scanning against the domains mentioned in the scope.

Unauthorised users were found to **have access to writable S3 Bucket** on the domain "**Sample-s3-bucket-1.democorp.com**", this **misconfiguration can facilitate** an attacker to have write access over the S3 bucket and can therefore facilitate an attacker to perform **data breaches** and **misuse the resource**.

Also, it was found that one of the **container images stores credentials and tokens in plain text** as environment variables. This can facilitate an **attacker to get access to applications and sensitive data** which might lead to **significant data breaches**.

Apart from this, **IAM (Identity Access Management) keys were found to be static** and no plan to rotate keys was found. As keys are used more and more in different scenarios and environments, the **chances of the keys being leaked increases**. If an unfortunate event occurs in which the keys are leaked, impact of such an event can be significant and **can result in unauthorised access, potential data breaches, compromised resources, and unauthorised usage** due to the exploitation of compromised or leaked keys.

Also, **S3 bucket's access logging** was found to be **disabled**, although it is not a serious issue but **access logging enables the ability to track requests** for access to the bucket which can help track the sources of request in case an unfortunate event occurs.

10. Key Strengths and Weaknesses

The following identifies the **key strengths** found during the assessment:

- Use of technologies that have no exploits available out in the open.

The following identifies the **key weaknesses** found during the assessment:

- Good security practices are not being followed.
- Use of outdated technologies.

11. Vulnerability Distribution Table

The following table illustrates the vulnerabilities found by findings and recommended remediations:

FINDINGS	SEVERITY	RECOMMENDATIONS
CPT-001: Writable S3 Buckets	Critical	Provide write access to specific buckets only.
CPT-002: ECR Image Weak Credential Storage	High	Do not use environment variables as storage for sensitive information.
CPT-003: No IAM User Access Key Rotation	Medium	Implement a plan to regularly rotate all IAM user access keys.
CPT-004: S3 Bucket Access Logging Disabled	Low	Enable access logging for the affected S3 buckets.
CPT-005: EC2 Instance Termination Protection Disabled	Info	Consider enabling EC2 instance termination protection for all affected instances.

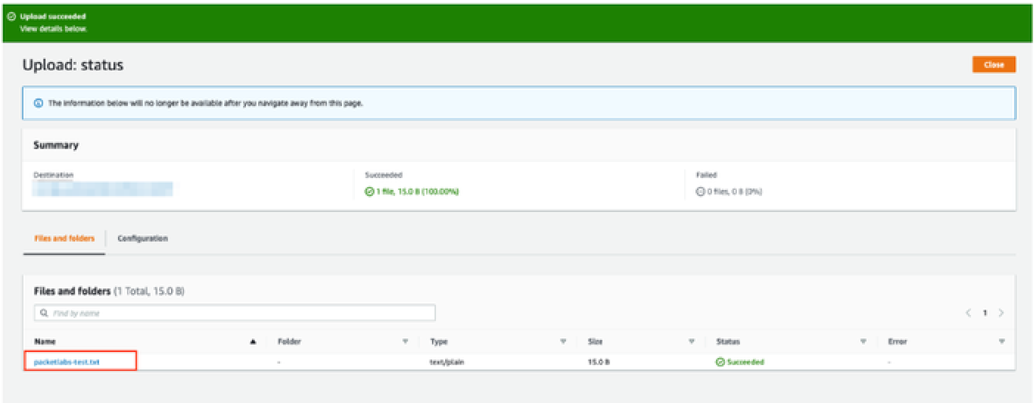
12. Cloud Penetration Testing Findings

CPT-001: Writable S3 Buckets (Critical)

DESCRIPTION:	During the testing of the cloud environment, it was found that the role tested has unrestricted privileges to write to S3 buckets. Writable S3 buckets allow an attacker to modify objects stored within which can be used to modify or upload scripts, workflow files, or source code files to introduce a backdoor to the cloud environment.
URL:	s3://Sample-s3-bucket-1.democorp.com
APPROACH:	Manual
TOOLS USED:	N/A
REFERENCES:	Amazon S3 Buckets

Evidence

The attached policy to the current user allows access to read all buckets and their stored objects. To avoid impacting production, none of the existing objects were overwritten. Instead, a sample file was uploaded to one of the buckets successfully



Upload succeeded
View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination: [redacted]

Succeeded: 1 file, 15.0 B (100.00%)

Failed: 0 files, 0 B (0%)

Files and folders (1 Total, 15.0 B)

Name	Folder	Type	Size	Status	Error
packetlabs-test.txt	-	text/plain	15.0 B	Succeeded	-

Fig 1: Uploaded text file to vulnerable S3 Buckets

Risk

- **Likelihood**

  A misconfigured S3 bucket can increase the likelihood of unauthorized users gaining write access.

- **Impact**

  Unauthorized write access can lead to data breaches, loss of sensitive information, malware distribution, regulatory non-compliance, financial losses, and reputational damage.

Remediation

Provide write access to specific buckets only when required. Revoke write privileges when they are no longer in use.

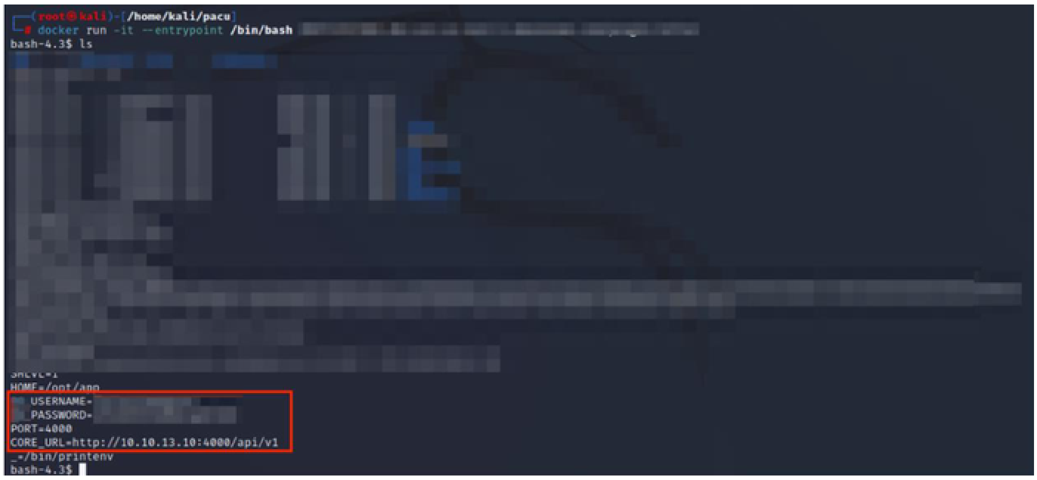
- **More Information**
  - Bucket Policies
  - S3 Access Control

CPT-002: ECR Image Weak Credential Storage (High)

DESCRIPTION:	During the testing of the cloud environment, it was found that one of the container images stores credentials and tokens in plaintext as environment variables. Credentials stored in environment variables are accessible by attackers once the image is successfully pulled.
URL:	democorp-ecr-image
APPTOACH:	Manual
TOOLS USED:	N/A
REFERENCES:	What is Amazon Elastic Container Registry?

Evidence

The image below shows the democorp-ecr-image having plaintext credentials and tokens stored in the environment variable. These credentials are used to authenticate to the local application which contains sensitive data.



```
┌──(root㉿kali)-[/home/kali/pacu]
└─# docker run -it --entrypoint /bin/bash [redacted]
bash-4.3$ ls
[redacted]
SHLVL=1
HOME=/opt/app
[redacted]_USERNAME=[redacted]
[redacted]_PASSWORD=[redacted]
PORT=4000
CORE_URL=http://10.10.13.10:4000/api/v1
_=/bin/printenv
bash-4.3$ 
```

Fig 2: Stored creds in ECR

Risk

- **Likelihood**

  There is a strong chance of encountering the ECR Image Weak Credential Storage issue, as developers might unintentionally store hardcoded credentials in images pulled from the registry. This is more likely in environments with inadequate security practices.

- **Impact**

  Compromised credentials from images could provide unauthorized access to applications with sensitive data. Malicious actors exploiting these credentials might lead to significant data breaches, loss of sensitive information, and potential legal and reputational repercussions.

Remediation

Do not use environment variables as storage for sensitive information and instead use a secrets manager to store sensitive data.

- **More Information**

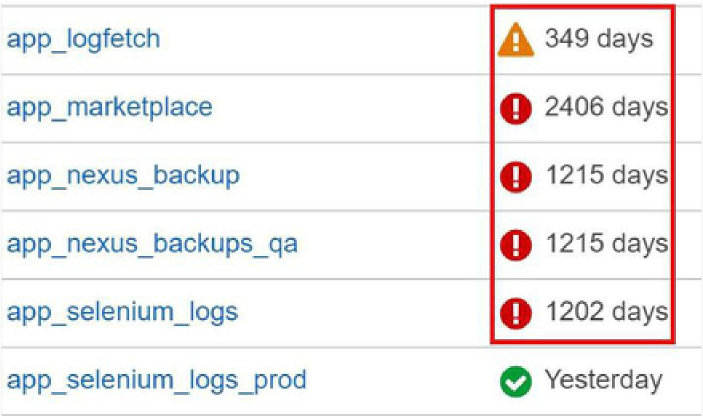
  - Authenticating Amazon ECR Repositories for Docker CLI
  - Private registry authentication - Amazon ECR

CPT-003 : No IAM User Access Key Rotation (Medium)

DESCRIPTION:	There is no plan to rotate IAM user access keys at regular intervals. By regularly rotating access keys, the chances of a set of keys being breached go down significantly. Over time, keys usually end up being used in more and more different places; this could be due to new computers, servers, employees, applications, or other similar things. This can increase the chance that someone malicious may discover them and abuse them.
URL:	IAM Users
APPROACH:	Manual
TOOLS USED:	N/A
REFERENCES:	Rotate Access Keys for IAM users

Evidence

This vulnerability was discovered by reviewing the "Access Key Age" setting for each IAM user. This indicated a large amount of time since the last key rotation was done. The screenshot shows a subset of users with long-lasting access keys; some over 1000 days old and one over 2400 days old.



app_logfetch	⚠ 349 days
app_marketplace	❗ 2406 days
app_nexus_backup	❗ 1215 days
app_nexus_backups_qa	❗ 1215 days
app_selenium_logs	❗ 1202 days
app_selenium_logs_prod	✓ Yesterday

Fig 3: Last rotated Key for IAM users

Risk

- **Likelihood**

  Not rotating IAM user access keys in AWS can lead to increased security risks and unauthorized access. If a key is compromised or leaked, it can be exploited by malicious actors to gain unauthorized access to AWS resources.

- **Impact**

  The impact of not rotating IAM user access keys in AWS includes an increased risk of unauthorized access, potential data breaches, compromised resources, and unauthorized usage due to the exploitation of compromised or leaked keys.

Remediation

Implement a plan to regularly rotate all IAM user access keys. It is suggested to rotate keys at least every 90 days, but 30 to 60 days would be even more secure.

- **More Information**

  - Managing access keys for IAM users - AWS Documentation
  - Automatically rotate IAM user access keys at scale with AWS Organizations and AWS Secrets Manager

CPT-004: S3 Bucket Access Logging Disabled (Low)

DESCRIPTION:	Access logging is not enabled for the affected S3 buckets. Access logging enables the ability to track requests for access to the bucket. The logs provide details about the incoming request and how it was responded to. There are no additional fees for enabling access logging, but the normal S3 storage charges occur for the stored logs.
URL:	s3://sample-bucket-2.democorp.com
APPROACH:	Manual
TOOLS USED:	NA
REFERENCES:	ServerLogs

Evidence

This vulnerability was discovered by reviewing the settings associated with the affected buckets and noting that access logging was disabled.

Risk

- **Likelihood**

  Disabling S3 bucket access logging increases the risk of unauthorized access, data breaches, and security incidents due to the lack of visibility into bucket activities.

- **Impact**

  Without access logs, it becomes challenging to trace, monitor, and investigate unauthorized access. This compromises incident response, hampers compliance audits, and diminishes the ability to demonstrate adherence to security standards.

Remediation

Enable access logging for the affected S3 buckets. This can be done through the web console by going to the options of an affected bucket, then the "Properties" tab, then clicking the "Server access logging" button.

- **More Information**
  - Enabling Amazon S3 server access logging
  - Logging requests using server access logging

CPT-005 : EC2 Instance Termination Protection Disabled (Info)

DESCRIPTION:	EC2 instance termination protection prevents instances from being terminated from the AWS console, Cloud, or CLI. This is used to prevent accidental or inappropriate instance termination by a user that doesn't have local access to the operating system.
URL:	prod-ec2-democorp
APPROACH:	Manual
TOOLS USED:	N/A
REFERENCES:	What is AWS EC2?

Evidence

This vulnerability was discovered by reviewing the termination protection setting for the affected EC2 instances.

Risk

- **Likelihood**

  The likelihood of EC2 Instance Termination Protection being disabled is Medium. This is due to the potential for human error or misconfiguration during routine instance management activities.

- **Impact**

  The impact of EC2 Instance Termination Protection being disabled can be significant. Without termination protection, instances become susceptible to accidental termination, potentially leading to data loss, service disruptions, and increased operational overhead.

Remediation

Consider enabling EC2 instance termination protection for all affected instances. This can be done through the EC2 console settings for each individual instance and in the launch configuration of new instances.

- **More Information**
  - AWS EC2 Enable Termination Protection

SECUREU

WE MAKE SECURITY ACCESSIBLE

Questions? Contact us at
Email : contact-us@secureu.in Phone : +91 8010450348