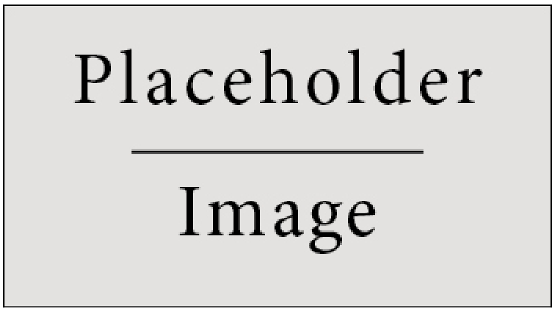

2024 Network Pentest Report

Prepared for The Cozy Croissant

Team [TEAM IDENTIFIER]

Report Issued: August 10, 2024

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to The Cozy Croissant or facilitate attacks against The Cozy Croissant. Team [TEAM IDENTIFIER] shall not be held liable for special, incidental, collateral, or consequential damages arising from the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on The Cozy Croissant’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

Changelog

v1.0	August 10, 2024	Report issued.

Table of Contents

1 Executive Summary

Team [TEAM IDENTIFIER] performed a security assessment of the internal corporate network of The Cozy Croissant on August 10, 2024. Team [TEAM IDENTIFIER]'s penetration test simulated an attack from an internal threat actor attempting to access systems within the The Cozy Croissant corporate network. This assessment aimed to discover and identify vulnerabilities in The Cozy Croissant's infrastructure and suggest methods to remediate the vulnerabilities. Team [TEAM IDENTIFIER] identified a total of 999 vulnerabilities within the scope of the engagement broken down as follows:

- 5 **Critical** vulnerabilities
- 3 **High** vulnerabilities
- 7 **Medium** vulnerabilities
- 3 **Low** vulnerabilities

The highest severity vulnerabilities allow potential attackers to **<BAD ACTIONS THAT COULD OCCUR HERE - FULL PARAGRAPH WITH HIGH-LEVEL DETAIL>**. To ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities in the systems within the scope. Any changes made to the environment during the testing period may affect the assessment results.

1.1 Testing Narrative

<An overview of the engagement, what the team tried that went well, and what didn't work. This should be tailored to the engagement>

1.1.1 Escalation Path

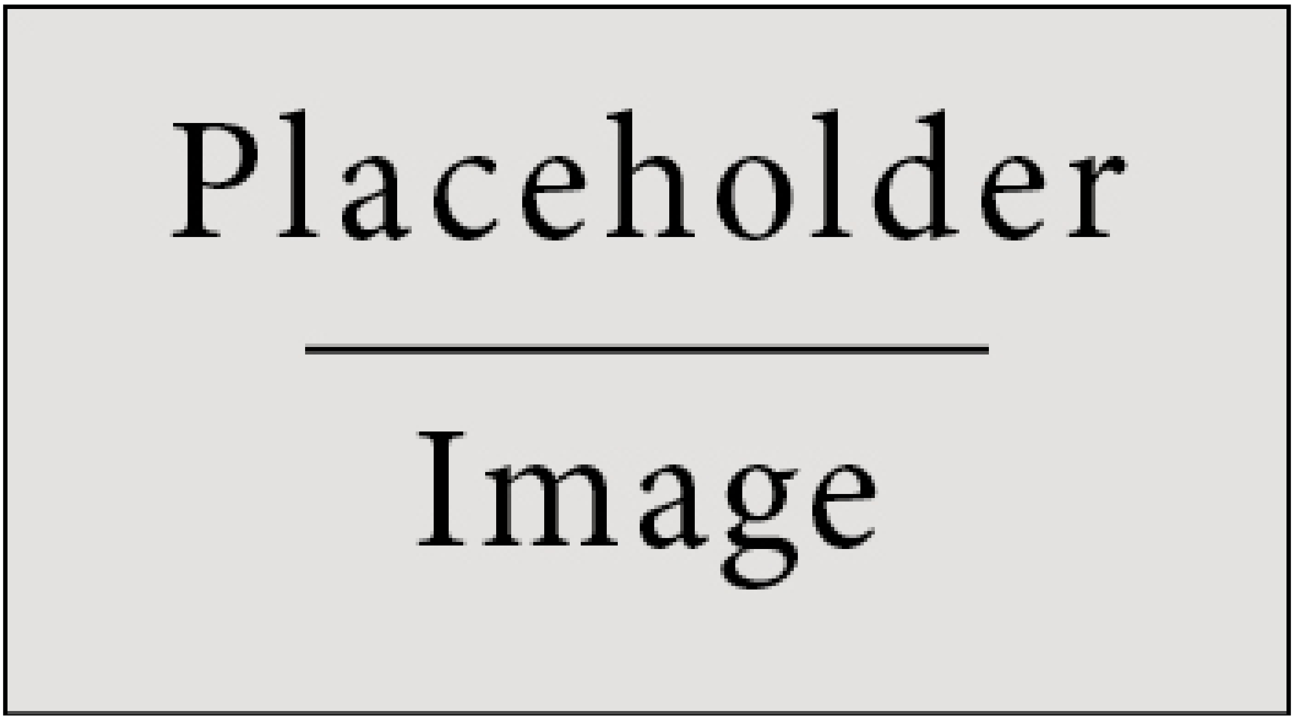

Figure 1: Escalation Diagram.

<Assuming the team obtained DA/high privileges, include a diagram showing the path taken, and explain an overview of the path here.>

1.2 Observed Security Strengths

Observation	Description
Network Segmentation	The network was super segmented and shit.
No Easily Guessable Passwords	I could not guessa da passwords.
Something Good Here	There are bugs under my skin.

1.3 Key Observations

TODO: put a cool table here

2 Engagement Information

2.1 Scope

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

Networks

Network	Note
10.0.1.0/24	Guest Network
10.0.2.0/24	Corporate Network

Other Assets

System	Type	Note
172.3.4.5	EC2 Instance	Cloud webserver
172.1.4.3	S3 Bucket	Super cool storage

2.2 Client Information

Client	Primary Contact	Approvers
The Cozy Croissant	Ted Striker, CEO	Ted Striker, Bill Cosby

3 Classification Definitions

Risk Classifications

Level	Description
Critical	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	These findings have no clear threat to the organization but may cause business processes to function differently than desired or reveal sensitive information about the company.

Sophistication Classifications

Level	Description
High	Exploitation requires a deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.
Medium	Exploitation methods are well-known and may be performed using public tools but require configuration. An understanding of the underlying system is required for successful exploitation.
Low	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.

Remediation Classifications

Level	Description
High	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Medium	Remediation may require minor re-configurations or additions that may be time-intensive or expensive.
Low	Remediation can be accomplished in a short amount of time, with little difficulty.

4 Assessment Findings

TCC1 – Test Finding

Risk	Sophistication	Remediation
Critical	High	Low

Observation

What did we find?

Affected Systems

- System 1
- System 2

Impact

Why is this bad, what can an attacker do with it?

Compliance

Does this have any compliance concerns?

Recommendation

How should this get fixed?

References

- website

Evidence

Screenshots and stuff here about how to replicate the vulnerability

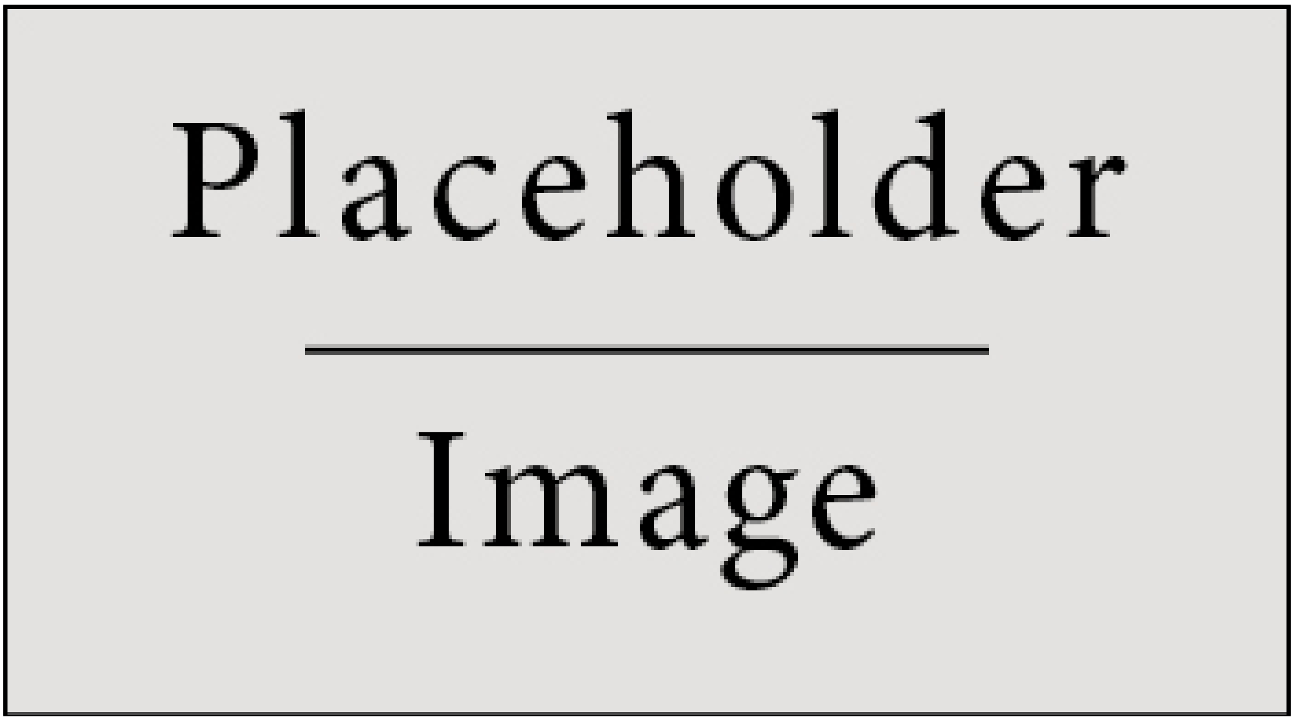

Figure 2: Escalation Diagram.

Appendices

A Tools Used

Tool	Description
BurpSuite	Tool for testing web applications
Sliver	Command and control framework
Nmap	Network and port scanner