1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain `email.92mountainview.com` using a Basic scan type. The analysis was initiated on May 31st at **23:00** and completed in **00h:10m:43s**. The tracking ID for this assessment is `0e5132922cef`. The scope of the work included a comprehensive evaluation of the domain's web application and infrastructure, focusing on identifying potential security vulnerabilities using OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **3 Medium-risk**, **2 Low-risk**, and **13 informational**. Key medium-risk findings include the detection of potentially insecure HTTP ports and sensitive subdomains, which could expose critical systems to unauthorized access. The shared hosting environment analysis revealed one host with medium interest due to shared domains, indicating a need for enhanced monitoring. SSL/TLS protocols are generally secure, with two endpoints using TLS **1.2**, but lacking TLS **1.3** support. No unusual port assignments or brute-force vulnerable services were detected, suggesting a stable network configuration. Immediate actions should focus on securing HTTP services and reviewing subdomain access controls to mitigate potential risks.

1.3 Issues Table

Title	Risk
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
Shared Hosting Environment Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:
The scan identified **2 open ports** on the IP address **76.223.17.250**. Port **80** is associated with an HTTP service that lacks encryption, posing a potential security risk if not redirected to HTTPS or if HSTS is not enabled.

Affected Assets:
- IP: **76.223.17.250**

Recommendations:
- Ensure that HTTP traffic is redirected to HTTPS. - Implement HSTS to enforce secure connections. - Regularly monitor and update server configurations to adhere to best security practices.

1.4.2 Subdomain Naming Security Assessment

Description:
A sensitive subdomain, `email.92mountainview.com`, was detected, which may provide access to critical systems and sensitive data. This subdomain is categorized as high risk due to its potential exposure of internal system details.

Affected Assets:
- Subdomain: `email.92mountainview.com`

Recommendations:
- Conduct a thorough review of access controls for sensitive subdomains. - Implement strict authentication and authorization measures. - Regularly audit subdomain configurations to prevent unauthorized access.

1.4.3 Shared Hosting Environment Analysis

Description:
The analysis revealed that the domain `email.92mountainview.com` is part of a shared hosting environment with **28 shared domains**, categorized as medium interest. This setup can lead to potential security risks due to shared resources.

Affected Assets:
- Hostname: `email.92mountainview.com`

Recommendations:
- Consider migrating to a dedicated hosting environment to reduce shared resource risks. - Implement network segmentation to isolate critical systems from shared environments. - Enhance monitoring of shared hosting environments for unusual activities.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to prioritize the implementation of HTTPS across all services, conduct regular audits of subdomain configurations, and consider transitioning to dedicated hosting environments where feasible. Additionally, adopting TLS **1.3** where possible will improve security and performance. Regular monitoring and updating of security configurations should be maintained to ensure compliance with best practices and emerging threats.