1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain `shibboleth.mintel.com` using a Basic scan type. The analysis commenced on November 28 at 05:00 and concluded after a duration of **4** hours, **9** minutes, and **29** seconds. The tracking ID for this assessment is `00fe99f60cbf`. The scope included a comprehensive evaluation of web applications and infrastructure, focusing on identifying high and medium-risk vulnerabilities.

1.2 Summary of Key Issues

The assessment identified **5 high-risk** and **6 medium-risk** issues. Below is a summary table of the findings:

Title	Risk
Shared Hosting Environment Analysis	High
Unusual Port Assignments Detected	High
SSL/TLS Protocols Security Assessment	High
Unencrypted HTTP Traffic Detected	High
Login Form Detection Analysis	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
API Surface Analysis	Medium
Hostname Density Analysis	Medium
SSL Certificate Expiration Analysis	Medium

1.3 Detailed Findings

1.3.1 Shared Hosting Environment Analysis

Description:
The analysis revealed a high-risk shared hosting environment with **257 shared domains** on `insights.mintel.com`. This configuration can lead to security risks as multiple domains share the same IP address, increasing the attack surface.

Affected Assets:
- `insights.mintel.com` with **257 shared domains**

Recommendations:
It is recommended to segregate critical services onto dedicated servers or use virtual private servers to minimize shared hosting risks. Implement strict access controls and continuous monitoring to detect unauthorized access.

1.3.2 Unusual Port Assignments Detected

Description:
A total of **10 high-risk unusual port assignments** were detected, indicating potential evasion of security controls or misconfigured applications. Services such as OpenVPN were found running on port **443**, which is typically reserved for HTTPS traffic.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING

Affected Assets:
-`globalsurveys.mintel.com` (34.252.175.198) -`relay1.uk.mintel.com` (5.148.99.39) -`relay1.us.mintel.c` (65.175.50.15) - Additional affected hosts listed in the detailed table.

Recommendations:
Review and standardize port assignments to align with best practices. Ensure that services are running on their designated ports and implement network segmentation to isolate critical services.

1.3.3 SSL/TLS Protocols Security Assessment

Description:
The assessment identified **23 endpoints** using deprecated TLS 1.0 and TLS 1.1 protocols, which are vulnerable to known attacks such as BEAST and lack modern cryptographic algorithms.

Affected Assets:
- Endpoints using TLS 1.0: **23** - Endpoints using TLS 1.1: **23**

Recommendations:
Upgrade all endpoints to support TLS 1.2 or higher, with a preference for TLS 1.3, to ensure robust encryption standards are maintained. Regularly review and update cryptographic configurations.

1.3.4 Unencrypted HTTP Traffic Detected

Description:
A total of **92 URLs** were found using unencrypted HTTP, exposing data to interception and eavesdropping risks.

Affected Assets:
- Sample URLs include `http://13.134.195.126:80`, `http://3.13.155.19:80`, among others.

Recommendations:
Implement HTTPS across all web applications to ensure data integrity and confidentiality. Utilize automated tools to enforce HTTPS redirection and HSTS policies.

1.3.5 Login Form Detection Analysis

Description:
The detection of **14 login forms** indicates potential exposure of authentication interfaces, which require security validation to prevent unauthorized access.

Affected Assets:
- URLs include `https://intranet.mintel.com:443`, `http://status.mintel.com:80`, among others.

Recommendations:
Conduct thorough security assessments of all login interfaces, ensuring strong password policies, multi-factor authentication, and secure transmission of credentials over HTTPS.

1.4 General Recommendations

To enhance overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, patch management, and user awareness training. Employing advanced threat detection and response solutions will further mitigate risks and protect critical assets from emerging threats.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING