1 Executive Security Assessment Report

1.1 Scan Details

- **Domain Analyzed:** pepsico.com
- **Tracking ID: 118376903605**
- **Type of Analysis:** Basic
- **Initiation Date and Time:** April 16, 03:45
- **Duration: 21** minutes and **17** seconds

1.2 Short Summary of Main Issues

The security assessment of pepsico.com identified several critical vulnerabilities. **182** email addresses and passwords were found leaked on the deep web, posing significant risks of phishing attacks and unauthorized access. The presence of high-risk shared hosting environments and open FTP ports further increases the potential for data breaches. Additionally, the analysis revealed a high service density across hosts, expanding the attack surface. Immediate actions are recommended to secure leaked credentials, close vulnerable ports, and enhance monitoring of shared hosting environments.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked on the Deep Web	High
Shared Hosting Environment Analysis	High
FTP Service	High
Unusual Port Assignments Detected	Medium
Nmap Port Scan Results Analysis	Medium
Service Density Analysis	Medium

1.4 Detailed Findings

1.4.1 Email Addresses and/or Passwords Leaked on the Deep Web

Description:
A total of **182** email addresses and passwords were discovered leaked on the deep web. This exposure poses critical security risks, including unauthorized access, phishing attacks, social engineering, and further data breaches. The credentials were found in multiple databases such as AntiPublic and BreachCompilation.

Affected Assets:
182 email addresses from pepsico.com employees.

Recommendations:
- Immediately reset passwords for all affected accounts. - Implement multi-factor authentication (MFA) across all user accounts. - Conduct security awareness training to mitigate phishing risks. - Monitor for any unauthorized access attempts using these credentials.

1.4.2 Shared Hosting Environment Analysis

Description:
The analysis identified high-risk shared hosting environments with **179** domains sharing the same IP address on `www.pepsico.com`, indicating potential risks associated with shared hosting.

Affected Assets:
- Hostnames: `pepsico.com`, `www.pepsico.com`

Recommendations:
- Consider migrating to a dedicated hosting environment to reduce risk. - Regularly audit shared hosting configurations for vulnerabilities. - Implement strict access controls and monitoring on shared servers.

1.4.3 FTP Service

Description:
An open FTP port was detected, allowing potential unauthorized access. This poses risks such as unauthorized file access, malicious uploads, and interception of cleartext data.

Affected Assets:
- IP Address: `45.223.17.132` - Hostname: `www.pepsico.com`

Recommendations:
- Disable FTP services if not required. - Use secure alternatives like SFTP or FTPS. - Implement strong authentication mechanisms and encryption for data in transit.

1.4.4 Unusual Port Assignments Detected

Description:
A total of **10** unusual port assignments were detected, with services running on non-standard ports or ports running unexpected services, which may indicate misconfigurations or attempts to evade detection.

Affected Assets:
- IP Address: `45.223.17.132` - Hostnames: `pepsico.com`, `www.pepsico.com`

Recommendations:
- Review and standardize port assignments according to best practices. - Conduct regular network scans to identify and rectify unusual port configurations. - Implement firewall rules to restrict access to necessary ports only.

1.4.5 Nmap Port Scan Results Analysis

Description:
The scan identified **18** open ports, some associated with potentially insecure services or protocols, suggesting exposure to unauthorized access and data interception.

Affected Assets:
- IP Address: `45.223.17.132`

Recommendations:
- Close unnecessary ports and services. - Implement intrusion detection systems (IDS) to monitor network traffic. - Regularly update software to patch known vulnerabilities.

1.4.6 Service Density Analysis

Description:
The host `45.223.17.132` was found with a high service density of **9** services, increasing the attack surface.

Affected Assets:
- Host IP: `45.223.17.132`

Recommendations:
- Reduce the number of services running on a single host. - Isolate critical services onto separate hosts or virtual machines. - Conduct regular audits to ensure minimal service exposure.

1.5 General Recommendations

To enhance overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, employee training on cybersecurity best practices, and continuous monitoring of network activities. Additionally, adopting a zero-trust architecture can further protect sensitive data and systems from unauthorized access.