



Penetration Testing Management Report

Prepared For: POST OFFICE
Target: Counter Training Office
Author: Jordan Williams
Date: 21 November 2022
Version: 1.0

Report Contents

1	HIGH LEVEL ASSESSMENT	3
2	EXECUTIVE SUMMARY	4
3	NEXT STEPS	5
4	REVISION HISTORY	6
5	DOCUMENT DISTRIBUTION LIST	6

The contents of this report belong to Post Office. The findings, information and recommendations in this document are for information purposes only and are based on a point in time assessment of the environment within scope. Nettitude, and the report's authors, accept no responsibility for any errors, omissions, or misleading statements, in this report, or for any loss that may arise for reliance on any information and opinions expressed. Nettitude recommends that all advice and recommendations are reviewed, a risk assessment conducted and change control processes followed before any remediation work is conducted. Nettitude does not hold any responsibility for any work conducted as a result of the recommendations provided in this report.

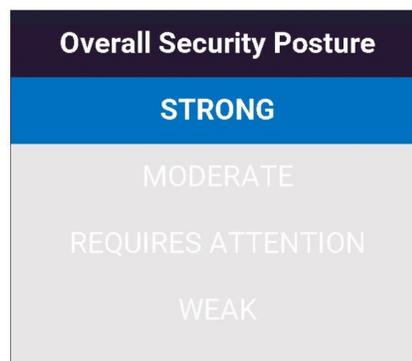
1 High Level Assessment

Post Office engaged with Nettitude in November 2022 in order to assess the overall security posture of their CTO environment.

Based on Post Office’s risk profile, primary security concerns and the vulnerabilities identified at the point of the engagement, Nettitude have found the CTO’s overall security posture to be **strong**.

Nettitude were able to:

- Identified strong level of security hardening
- Identify IP addresses of the Kiosks
- Determine that it was not possible to elevate privileges



Vulnerabilities by Severity

Critical	0
High	0
Medium	0
Low	0

Constraints and Limitations

No limitations were encountered during the engagement.

2 Executive Summary

In November 2022, Post Office engaged with Nettitude to carry out a black box thick client breakout test against the kiosk devices located in the counter training office. The environment was found to be made up of six Windows computer's that were security hardened and connected to the network.

During the assessment, Nettitude connected a keyboard, mouse, and a number of other devices to attempt to interact with the computers. Nettitude found that even when using alternative input devices that it was not possible to break out of the kiosk application running on the device or gain access to the underlying operating system.

Despite being unable to gain access to the host or elevate privileges during this test, Nettitude believe it would be worthwhile testing the system from the position of a compromised user account for the host systems to simulate what would be possible, for instance, if a 3rd party supplier had been compromised as this may highlight vulnerabilities that are present and were not found on this test.

Nettitude are available for additional debriefs upon request and Nettitude consultants are available for post-test remediation advice and guidance.

3

Next Steps

Nettitude recommends that Post Office perform the following post engagement activities in the order of priority indicated.

	Activity	Description	Priority
1	Debrief from Nettitude	Nettitude will deliver a formal debrief to Post Office in order to ensure that the findings of this engagement have been fully comprehended and to help assist in the formulation of a remediation plan.	++++
2	White Box Security Assessment	Build review of the kiosks systems with an administrator user account for the host system.	+++
3	Code Review	Full code review of the kiosk application	++
4	Retest	It is important to retest systems on a regular basis in case they are affected by newly discovered vulnerabilities of if changes are made to the host or application that could affect the overall security of the device.	+

4

Revision History

Version	Issue Date	Issued by	Comments
0.1	21 November 2022	Jordan Williams	Initial Draft
0.2	29 November 2022	Dalton Wright	Quality Assurance
1.0	30 November 2022	Jordan Williams	Final version

5

Document Distribution List

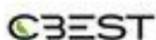
Nettitude	Name	Title
	Jordan Williams	Managing Principal Security Consultant
	Dalton Wright	Quality Assurance
	Tom Jordan	Account Manager

Post Office	Name	Title
	Mark J Cunningham	Security Risk Manager
	Julian Higgs	Security Assurance and Governance Specialist
	Khushtar Hosenie	Risk, Security & Data Governance Manager



Nettitude Penetration Testing Services

www.nettitude.com/penetration-testing/



NETTITUDE

AN LRQA COMPANY

UK Head Office

Jephson Court, Tancred
Close, Leamington Spa,
CV31 3RZ

Americas

50 Broad Street,
Suite 403, New York,
NY 10004

Asia Pacific

18 Cross Street,
#02-101, Suite S2039,
Singapore 048423

Europe

Leof. Siggrou 348
Kallithea, Athens, 176 74

GRO

Follow Us



solutions@GRO

www.nettitude.com