Penetration Test Summary Report

Prepared for:

Mark Houpt
Edge Hosting, LLC
120 East Baltimore St
Suite 1900
Baltimore, MD, 21202

Prepared by:

EIT Federal Cloud Services
3040 Williams Drive, Suite 400
Fairfax, VA 22031
703-568-4400

April 27, 2018
Service Order:-DataBank

EIT 3PAO Assessment Team

Practice Manager

Kris Martel, CISSP, CRISC, CISM, CGEIT, CCAH, MCSE
Executive Vice President of Operations
(540) 326-6929
kris.martel@eit2.com

Practice Director

Martin Rieger, CISSP, CCSP, CISA, CRISC, CISM, GSLC, MCSA
Director, Cyber Security & Risk Management
703-568-4400
martin.rieger@eit2.com

Assessor

Harrison Cook, C|EH, CCSP, SEC+CE
Senior Technical Expert, Penetration Tester
(571) 320-0132
harrison.cook@eit2.com

Table of Contents

Tables

Figures

1. EXECUTIVE SUMMARY

1.1 Project Overview

This penetration test has been performed to assess the Edge CloudPlus (IaaS/PaaS) across each of the required attack vectors as defined by FedRAMP for cloud-based information services. The penetration test has been developed and performed based solely on the asset list for in-scope systems. EIT engaged with DataBank to perform the penetration test of the CloudPlus (IaaS/PaaS) from September 17th, 2017 – October 31st, 2017. A second assessment was performed from March 26th, 2018 through April 21st 2018. On completion of each penetration test, the raw test reports were provided to the DataBankCP team for review and comment. This summary report includes the findings based on our observations and results for the testing conducted.

1.2 Summary of Scope and Attack Scenarios

The assets in scope for this engagement were pulled from the Integrated Inventory Workbook that was developed as part of the "*DataBank CloudPlus System Security Plan (SSP) 2017.04 dated 1 Oct 2017*" as the list of assets that are in scope for the assessment.

A follow-up penetration test was performed on new components brought into the boundary for the DataBank CloudPlus Infrastructure as a Service and Platform as a Service offering. The new components constitute DataBank's Security Stack. A separate management enclave within DataBank's internal management network.

Penetration testing was performed using Metasploit Pro, with authenticated Nessus discovery, vulnerability, and policy scan reports pre-loaded. The DataBank CloudPlus environment is presented within a VMWare virtualization infrastructure. Traditional discovery methods do not always effectively work in virtualized environments, therefore Emagine IT requested DataBank perform discovery using their instance of Tenable.IO (Nessus) during a shoulder-surfing session. Discovery was run for each of the documented subnets for verification that only the approved components documented in the integrated system inventory were present.

EIT performed the internal penetration test from a private IP on the Penetration testers LAN. It should be noted that EIT was issued Virtual Private Network (VPN) credentials by DataBank to remotely perform internal testing on the customer instance in addition to the administrative endpoints. It should also be noted that the IP's in scope were on different subnets so traditional ARP poisoning, NBNS spoofing or other MITM attack vectors could not be used as methods for breaching into a customer tenant space from the management backend and vice-versa.

In addition, the assets being offered for testing are primarily infrastructure and platform support services. The DataBank SSP identifies application and database configurations as customer responsibilities with DataBank support, at customer request, as needed for specific customer builds.

The Nessus.IO vulnerability scan results revealed zero findings that were exploitable within the DataBank, Security, DMZ, and Customer Instance subnets. Metasploit Pro was used for discovery and scanning of the endpoints documented in the system inventory provided by DataBank, and to automatically select the appropriate attacks to be performed. External testing was performed by EIT from a private IP on the penetration testers LAN.

For testing purposes, a multi-factor account and soft-token was issued to the penetration tester by DataBank.

Discovery scanning and penetration testing activities included external unauthenticated attacks against DataBank's DMZ based assets. Internal testing was performed in addition to internal and external technical testing, EIT also performed social engineering tests on the DataBank personnel assigned responsibilities and access rights to the CloudPlus. This was performed by sending a carefully crafted email to the DataBank personnel, containing a link and requesting the user to click the link within the email body. All users who clicked on the link were recorded by EIT's social engineering application. The results have been provided in this report.

The attack scenarios used in the DataBank penetration test were designed to provide a realistic attack surface. The scenarios are also based on the FedRAMP Penetration Test Guidance, Version 1.01, July 6th, 2015. Often, there are multiple potential paths to gain access to critical data and systems. The CloudPlus environment defined in the System Security Plan (SSP) is the secure network that our attacks attempted to penetrate.

1.3 Summary of Findings

The overall risk to the assets in scope is determined to be **Moderate**. Although there were identified vulnerabilities present within the DataBank CloudPlus environment when credentialed scans were run prior to the penetration test phase, successful exploit of those vulnerabilities was hampered by active inline intrusion detection and prevention. Information gathered during discovery and fingerprinting was utilized to build and launch multiple exploits based on any known weakness associated with the exposed port, service, or identified application or platform present on each of the assets. At no time during the penetration test was EIT able to gain unauthorized access to any systems, exploit any vulnerabilities or discover information that led EIT to believe the IP addresses that were tested were in an insecure environment. The security testing included penetration tests against the defined environment to proactively discover flaws, weaknesses and vulnerabilities.

All testing for this project was done in accordance with FedRAMP security requirements and the Rules of Engagement (RoE) agreed upon by DataBank and Emagine IT. The objective of this service was to identify and safely exploit vulnerabilities which could lead to critical service interruption, destruction of facilities or compromise of sensitive systems and data.

7. ACRONYMS

Acronym	Definition
3PAO	Third Party Assessment Organization
AO	Authorizing Official
API	Application Programming Interface
ARP	Address Resolution Protocol
CA	Certificate Authority
CERT	Computer Emergency Response Team
CIRT	Consumer Incident Response Team
CMVP	Cryptographic Module Validation Program
CP	Contingency Planning
CSP	Cloud Service Provider
CUI	Confidential Unclassified Information
DAA	Designated Approving Authority
DMZ	Demilitarized Zones
DNS	Domain Name System
DoS	Denial of Service
DHS	Department of Homeland Security
E-Authentication	Electronic Authentication
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
HTTP	Hyper Text Transport Protocol
IAP	Internet Access Points
IaaS	Infrastructure as a Service
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
ISSO	Information System Security Officer
JAB	Joint Authorization Board
LAN	Local Area Network
MiTm	Man in the Middle
NBNS	NetBIOS Name Service
NIST	National Institute of Standards and Technology

Acronym	Definition
NIST-SP	NIST Special Publication
NLA	No Logical Access
NP	Non-Privileged
OMB	Office of Management and Budget
Priv	Privileged
PaaS	Platform as a Service
P-ATO	Provisional Authorization to Operate
PDS	Protective Distribution System
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMO	Program Management Office
POA&M	Plan Of Action & Milestones
RA	Risk Assessment
RoE	Rules of Engagement
SaaS	Software as a Service
SAP	Security Assessment Plan
SAR	Security Assessment Report
SLA	Service Level Agreement
~~**SOC**~~	Security Operations Center
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSP	System Security Plan
TCP	Transmission Control Protocol
TLS	Transport Layer Security
US-CERT	U.S. Computer Emergency Response Team
UDP	User Diagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network