Confidential

Vulnerability Assessment & Penetration Testing Report for DinoBank

November 22-23, 2019

"Banking that's never prehistoric"

Assessors: [redacted]
Email: [redacted]

Disclaimer

The information contained in this document is confidential, privileged, and is available only for the intended recipient. This document, including any of the information provided, may not be used, published, or redistributed without the prior written consent of [redacted] and DinoBank.

Table of Contents

Purpose of Report

The purpose of the following report is to provide an overview of DinoBank's security posture by outlining the vulnerabilities and risks faced by the organization. The audience of this report is targeted towards a wide range of positions, including executives, management, administrators, analysts, IT specialists, and security personnel.

Section	Intended for
Executive Summary	CEO, CFO, etc.
Business Impact Analysis/Assessment	CIO, CISO, Compliance Officers, Senior Managers
Findings	Technical Personnel, Analysts
Recommendations	Project Managers, CIO, CISO

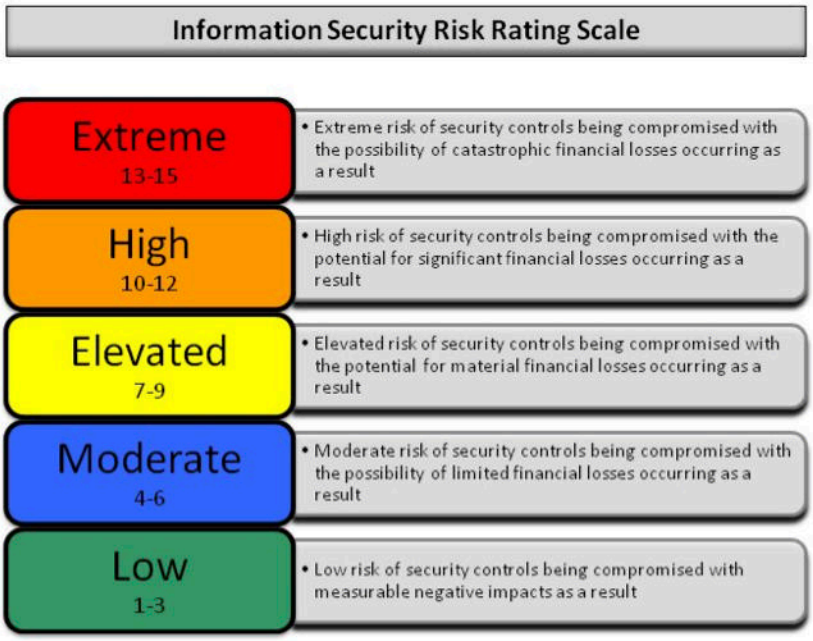
The report's appendices will include the following:

- Exploitations: Sensitive information that shows techniques used to identify vulnerabilities
- Findings: Each finding that was exploited has its own appendix with a screenshot of the launched attack on each host affected by the findings

[redacted]

Executive Summary

DinoBank Security Risk Rating: 10



After concluding DinoBank's penetration test, [redacted] has given DinoBank an overall security risk rating of **High.** The following rating was given due to the number of security vulnerabilities found on DinoBank's corporate network.

During our test against DinoBank's enterprise networks, [redacted] identified several areas of concern such as the widespread usage of plaintext/weak credentials. The usage of these credentials allowed our team to access one of DinoBank's production database servers. In this server, one of our testers discovered personally identifiable information, card data, and online banking account logins. The discovery of this database poses a significant risk for DinoBank as this might cause significant financial and legal repercussions from regulations such as the Gramm-Leach-Bliley Act or the NYS DFS 23 NYCRR 500.

It is essential that DinoBank remediate the findings found in this report to address many of the MOU concerns from the Gotham Department of Banking. Successful remediation of the vulnerabilities will allow DinoBank to continue its Banking operations. As part of our penetration testing service, the report includes remediation recommendations for the discovered vulnerabilities and a detailed action plan to strengthen DinoBank's security operations.

Objectives of Engagement

The objective of the engagement was to evaluate the overall security of DinoBank enterprise networks and to satisfy DinoBank's MOU requirements for the Gotham Department of Banking. The penetration test would highlight any issues along with the potential business impact that could arise from cyber-attacks from various threat actors. As part of our assessment, [redacted] has provided recommendations that will assist your organization in implementing a strategic remediation action plan.

Scope of Engagement

The following IP ranges are in scope for the penetration test:

- 10.0.1.0/24
- 10.0.2.0/24
- 10.0.10.0/24
- 10.0.11.0/24
- 10.0.12.0/24

Additional systems in scope for the penetration test:

- DinoBank ATM Machine
- IVR DID Phone
- Phone # 585-371-6793
- Tax ID (SSN) 304-40-7813
- PIN 1337

The following IP range is not in the scope for the penetration test:

- 10.0.254.0/24

Timeline of Engagement

[redacted] engagement with DinoBank started on November 22, 2019, and ended on November 24, 2019.

- November 22nd, 2019
  - 7:00 PM DinoBank Drive Access Allowed
  - 7:30 PM - 9:45 PM Start of Penetration Test (Direct Access)
- November 23rd, 2019
  - 8:15 AM - 6:00 PM Penetration Test (Direct Access)
  - 6:00 PM DinoBank Drive Access Revoked
  - 9:00 PM DinoBank Drive Access Allowed
- November 24th, 2019
  - 2:00 AM Submission of Penetration Testing Report/Presentation
  - 8:00 AM Board Presentation

Risk Classification Methodology

In order to effectively convey the risk of DinoBank's systems as assessed by [redacted] we have created a risk matrix scale as shown below. This scale offers a visual representation of the risk, impact, likelihood and remediation effort required of the systems that are critical to DinoBank. By providing the following risk matrix template, [redacted] hopes to be able to effectively define what our risk classification levels entail.

Risk Matrix

Likelihood/ Risk	Low Risk	Medium Risk	High Risk	Critical Risk
Critical Likelihood	High	High	Critical	Critical
High Likelihood	Medium	High	High	Critical
Medium Likelihood	Medium	Medium	High	High
Low Likelihood	Low	Medium	Medium	High

Risk

Critical	Improper handling and storing of PII, records, DDoS attack, ransomware, Cross-Site scripting, SQL injection
High	Unsupported operating system, insecure open ports, unpatched applications
Medium	Server or network downtime
Low	Memory scraping, change security management team

Impact

Critical	Loss of confidential data which can lead to damage reputation, customer loss, and legal regulatory repercussions
High	Destruction of data that could lead to company downtime and lost work
Medium	Obstruction of data that could lead to employee and customer dissatisfaction and frustration
Low	Loss of logging data that could lead to potential questions when attempting to determine accountability

Likelihood

Critical	Imminent occurrence based on the current security posture
High	High likelihood of occurring based on the current security posture
Medium	Medium to a low likelihood of occurring based on the current security posture
Low	Not likely to happen based on the current security posture

Remediation Effort

Critical	Significant monetary, personnel, training and operation disruption. It is advised that you do not hold this event without prior consultation with upper management
High	Considerable monetary, personnel, training and operational disruption. May require outside help.
Medium	Low monetary, personnel, training, and operational disruption
Low	Little to no impact on current operations

Business Impact Analysis

This section is an extension of the executive summary report. An overview of the top business-impacting vulnerabilities and potential ramifications are laid out below.

Risk of Insider Threat

The safety of DinoBank customer's information is a critical portion of your organization. During the extent of [redacted] penetration test, we discovered many insecure systems and services available to individuals inside the corporate network. These vulnerabilities could result in the loss of customer information and corporate data. The majority of the insider threat concerns arose from system misconfigurations of services and ports. Machines with misconfiguration could be accessed by any members of the internal network and could be misused. In additional, [redacted] notices a lack of proper network segmentation which exposes the network to potential access abuse.

MOU Satisfaction

The Memorandum of Understanding that DinoBank is currently being investigated for is focused on enforcing proper security controls within the company.

1. Lack of Security Governance
    a. DinoBank lacks accountability and oversight to ensure that risks are adequately mitigated while ensuring that the correct controls are implemented to mitigate risk.
2. Banking Core Weakness
    a. Outdated software leaves vulnerabilities in the core function of DinoBank.
    b. Default credentials in DinoBank's system enable the opportunities of a breach.
    c. No segmentation of networks or databases.
    d. Passwords aren't aligned with the corporate password policy.
3. Poor Management
    a. Insufficient communication between the members of the board in directing the penetration test.
    b. Unclear tracking of employees in the internal systems.
    c. Miscommunication in the testing of the ATM, causing confusion in the penetration test.

   d. Employes not restricted from accessing the penetration test, causing engagement concerns.
4. Insufficient Audit Coverage
   a. Use of company resources for purposes other than intended.
   b. Lack of security control testing
   c. Lack of security control enforcement

Regulations and Compliance

DinoBank is a national bank that provides a variety of different account services such as consumer accounts, business accounts, and crypto-based assets. Due to the nature of DinoBank's business, DinoBank has several compliance requirements such as:

- Gramm-Leach-Bliley Act
  - Requires financial institutions to explain how they share and protect their customers' private information.
- NYS DFS 23 NYCRR 500
  - The 23 NYCRR 500 regulation requires financial organizations to be compliant with a set of 22 provisions to protect the organization against nation-states, terrorist organizations and independent criminal actors.
- Payment Services Directive 2 (PSD2)
  - Bank and third-party provider (TPP) have to comply with Payment Services Directive 2 which require these organizations to enforce strong customer authentication and mobile app security.

From our assessment, DinoBank is failing many of the mandatory controls required by the different regulations stated above. By failing to meet the security controls, DinoBank may risk facing regulatory fines or seize of banking operations.

Third-party service provider management

During [redacted] assessment, our team worked with DinoBank's third-party service provider. In particular, [redacted] interacted with ATM contractors for DinoBank. During our interaction, [redacted] observed a lack of security awareness from DinoBank's ATM contractors. As an example, the contractors left the ATM configuration access open for the ATM machine during routine ATM maintenance. [redacted] also observed improper clean-up at the end of the maintenance cycle. The lackluster behavior from the ATM contractor team is a huge security vulnerability for DinoBank as the improper care of the ATM machine could allow for a variety of ATM-based attacks

such as terminal tampering, shimming, or jackpotting. The ATM also accepts any pins for transactions entered. This creates a huge security risk as anyone could just enter in a card they found and immediately withdraw money from it.

Exfiltration of sensitive data

During the assessment, [redacted] discovered a Postgres database server containing sensitive information in the categories of customer data, employee data, and banking card data. The discovery of this database poses a huge risk to DinoBank as the bank could face a cybersecurity breach. The data discovered in the database was also not encrypted which makes it accessible for attackers to exfiltrate and sell the personal information on the black market. In the event of a breach, DinoBank will also face many regulatory and publicity issues.

Technical Summary

[redacted] offensive security team adheres to the penetration testing execution standards 1.0 (PTES). The PTES is a cybersecurity framework with operating procedures for a penetration test. The framework assists the penetration test in ensuring that all basis of a test is covered.

The penetration test execution standard consists of seven (7) sections: pre-engagement, intelligence gathering, thread modeling, vulnerability analysis, exploitation, post-exploitation, and reporting.

The PTES methodology provides the highest level of feedback and analysis while being as unobtrusive as possible to maintain testing standards.

1. [redacted] will begin with network enumeration by running a series of network scans to discover systems in the proposed testing scope. After the scanning phase, a vulnerability scan will be configured to uncover any existing system flaws for usage in the penetration test. [redacted] will also retest any of the previously discovered vulnerabilities found in the initial penetration test.

2. After compiling the system information. [redacted] will begin exploiting the machine depending on the discovered vulnerabilities, services, and flaws. Once inside the internal network, [redacted] will attempt to explore the network and look for sensitive data that could be potentially exfiltrated. [redacted] will also utilize any lateral movement and privilege escalation techniques.

3. Throughout the entire penetration testing process, [redacted] will document all findings and techniques to prepare an executive report and presentation. The report will outline the entirety of our findings, risk analysis, and remediation recommendations to improve the security posture of your organization.

Penetration Testing Tools

Tools	Purpose
Owasp Zed Attack Proxy Project	Discover security vulnerabilities in web applications
Burp Suite	Security testing of web applications
Owasp Dirbuster/Dirb/GoBuster	Designed to brute force website directories
OpenVas	A security framework for vulnerability scanning/management
Nmap	Network Scanner/Exploration/Enumeration
AutoRecon	Automated network enumeration tool
Legion	Semi-automated network penetration testing
Metasploit	Penetration testing framework
Searchsploit/ExploitDB	Exploit database repository
SMBClient	Samba Client on Linux to test SMB
Nikto	Outdated web server scanner
Enum4Linux/Enum.exe	Enumeration tool for Windows and Samba
Bitvise SSH/Putty/OpenSSH/RDP	Remote connectivity to Windows and Linux machines
Discover Scripts, Wordhound, Prowl, Skiptracer, Tinfoleak, EmailHarvester, Spiderfoot, Stegosuite, Steghide, Exiftool, Sherlock	OSINT Tools

Availability of Services

[redacted] understands the business impact of server downtime; [redacted] will work extensively with DinoBank to maintain service uptime to sustain continuous business functions. During the penetration test, [redacted] took the utmost care in only performing non-disruptive scans against DinoBank's network. Due to the sensitive nature of banking data, we understand that careful testing is necessary as any data loss is potentially unrecoverable. To be transparent with our evaluation and to provide DinoBank with the highest level of service possible, [redacted] will take the following steps to ensure minimal disruption to DinoBank's services.

1. All reconnaissance tools will be using non-intrusive scan settings to ensure that systems are not overloaded. i.e. DDOS

2. In the exploitation phase, only the usage of professionally vetted and researched exploits. This process will include exploit code review, and custom exploits modification.

3. [redacted] will treat compromised systems with caution, taking note to ensure minimal system interruption from stopped or restarted services.

4. [redacted] will document and revert any changes performed by [redacted] at the end of the assessment. The procedure will ensure that the discovered vulnerabilities are not available to external actors.

5. In the event that [redacted] interrupts a running system or service, [redacted] will take immediate action to notify DinoBank security and information technology teams to restore business functionality in the quickest manner possible.

Network Penetration Test Findings

During our penetration testing assessment, [redacted] discovered vulnerabilities found in the system from the October assessment that were not remediated such as anonymous FTP login, outdated services, and weak cipher encryption.

Beyond validating the previous vulnerabilities, [redacted] discovered new vulnerabilities on the network with outdated services, unsecured web applications, and default credentials. These vulnerabilities could open DinoBank to the potential of a data breach.

In the analysis of a Postgres database that we found, [redacted] found plaintext personal identifiable information along with banking card data. In the assessment, [redacted] notified members of DinoBank's executive board to respond to these findings.

FTP Anonymous Login

File Transfer Protocol (FTP) allows clients to access different file servers within the infrastructure. The FTP server is misconfigured and may cause a lot of trouble if exploited. By allowing anonymous users to connect to FTP, the company risks the ability to properly log its assets and prevent unauthorized data manipulation.

Risk Rating

Risk	Impact	Likelihood	Remediation
Medium	Medium	Medium	Low

Infiltration Technique

Once the Nmap scan completed, our team discovered an FTP service running on nationals-t10-corp-corp-wsus-01.c.infra-test-environment.internal (10.0.1.12). Upon connection, we were able to use an anonymous login to gain access to the service. We were then able to navigate the file system to view and acquire files with world-readable permissions, such as Suricata and win10pcap logs.

Remediation

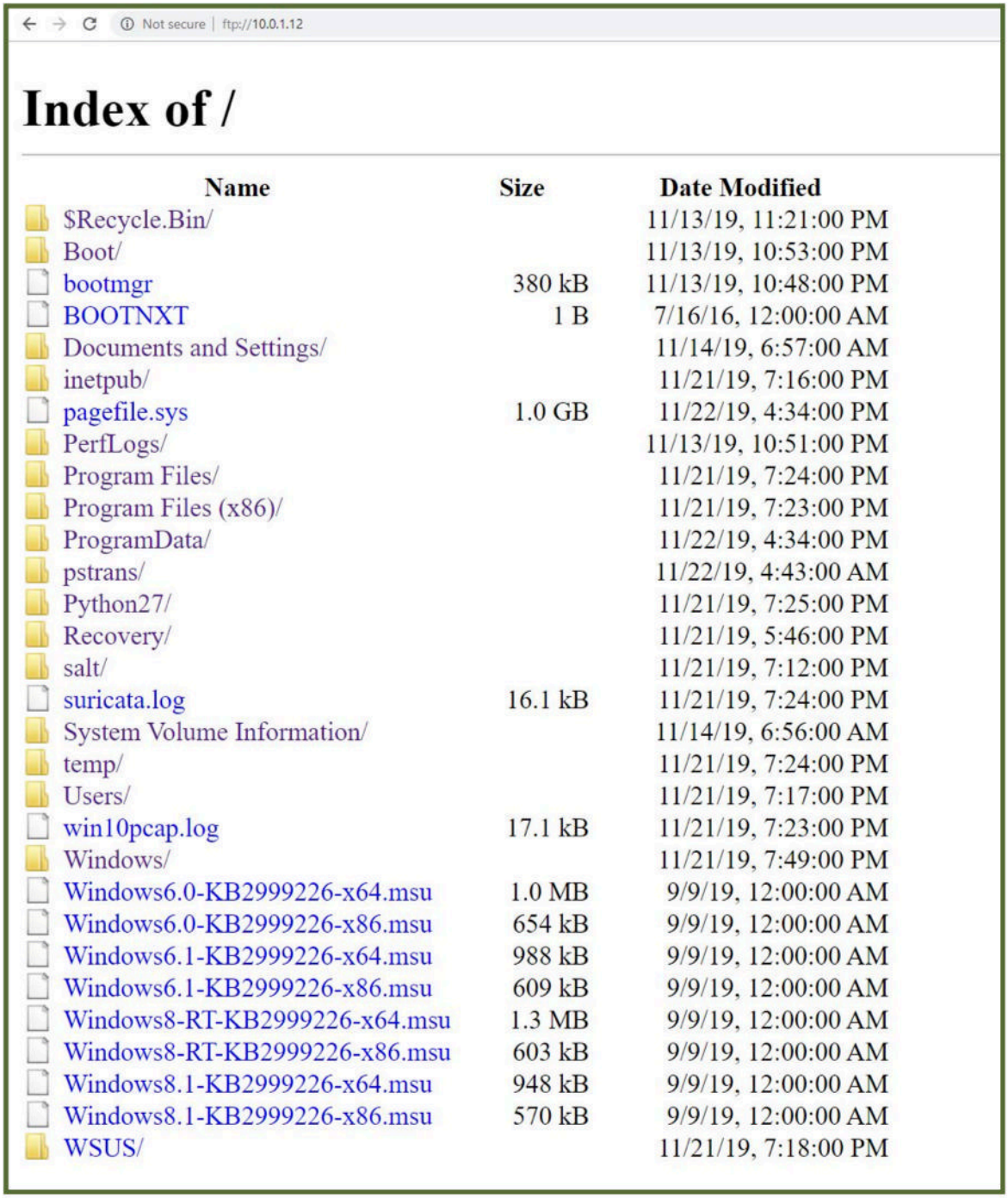
To remediate this attack our team recommends disabling FTP anonymous login. This can be done through the Internet Information Services (IIS) Manager, by selecting server, followed by FTP authentication, and making sure “Anonymous Authentication” is unchecked/disabled.

Assets Affected

- 10.0.1.12 ([redacted]-corp-corp-wsus-01.c.infra-test-environment.internal)

Evidence

```
/envs/nationals-cptc [redacted]/kali03 @~ # ftp 10.0.1.12
Connected to 10.0.1.12.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (10.0.1.12:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
```



Not secure | ftp://10.0.1.12

Index of /

Name	Size	Date Modified
$Recycle.Bin/		11/13/19, 11:21:00 PM
Boot/		11/13/19, 10:53:00 PM
bootmgr	380 kB	11/13/19, 10:48:00 PM
BOOTNXT	1 B	7/16/16, 12:00:00 AM
Documents and Settings/		11/14/19, 6:57:00 AM
inetpub/		11/21/19, 7:16:00 PM
pagefile.sys	1.0 GB	11/22/19, 4:34:00 PM
PerfLogs/		11/13/19, 10:51:00 PM
Program Files/		11/21/19, 7:24:00 PM
Program Files (x86)/		11/21/19, 7:23:00 PM
ProgramData/		11/22/19, 4:34:00 PM
pstrans/		11/22/19, 4:43:00 AM
Python27/		11/21/19, 7:25:00 PM
Recovery/		11/21/19, 5:46:00 PM
salt/		11/21/19, 7:12:00 PM
suricata.log	16.1 kB	11/21/19, 7:24:00 PM
System Volume Information/		11/14/19, 6:56:00 AM
temp/		11/21/19, 7:24:00 PM
Users/		11/21/19, 7:17:00 PM
win10pcap.log	17.1 kB	11/21/19, 7:23:00 PM
Windows/		11/21/19, 7:49:00 PM
Windows6.0-KB2999226-x64.msu	1.0 MB	9/9/19, 12:00:00 AM
Windows6.0-KB2999226-x86.msu	654 kB	9/9/19, 12:00:00 AM
Windows6.1-KB2999226-x64.msu	988 kB	9/9/19, 12:00:00 AM
Windows6.1-KB2999226-x86.msu	609 kB	9/9/19, 12:00:00 AM
Windows8-RT-KB2999226-x64.msu	1.3 MB	9/9/19, 12:00:00 AM
Windows8-RT-KB2999226-x86.msu	603 kB	9/9/19, 12:00:00 AM
Windows8.1-KB2999226-x64.msu	948 kB	9/9/19, 12:00:00 AM
Windows8.1-KB2999226-x86.msu	570 kB	9/9/19, 12:00:00 AM
WSUS/		11/21/19, 7:18:00 PM

Anonymous FTP File Contents

Outdated Suricata

Suricata is a network threat detection engine, acting as an (IDS) intrusion detection system and (IPS) intrusion prevention system. An outdated version of Suricata was found on the network, version 4.0.5-1. The current version is 5.0.0., using outdated IDS software could put a network at risk by not updating to the latest version and most advanced version of the software. Outdated Suricata version 4.0.5-1 is also vulnerable, leaving an attack vector open for attackers. Detection bypass, out-of-bounds read, and integer overflow/wraparound are the vulnerabilities for the outdated version of Suricata.

Risk Rating

Risk	Impact	Likelihood	Remediation
Medium	Medium	Low	Low

Infiltration Technique

Enumeration utilizing the anonymous FTP access led to the discovery of the Suricata installation log file in the C:\: drive directory.

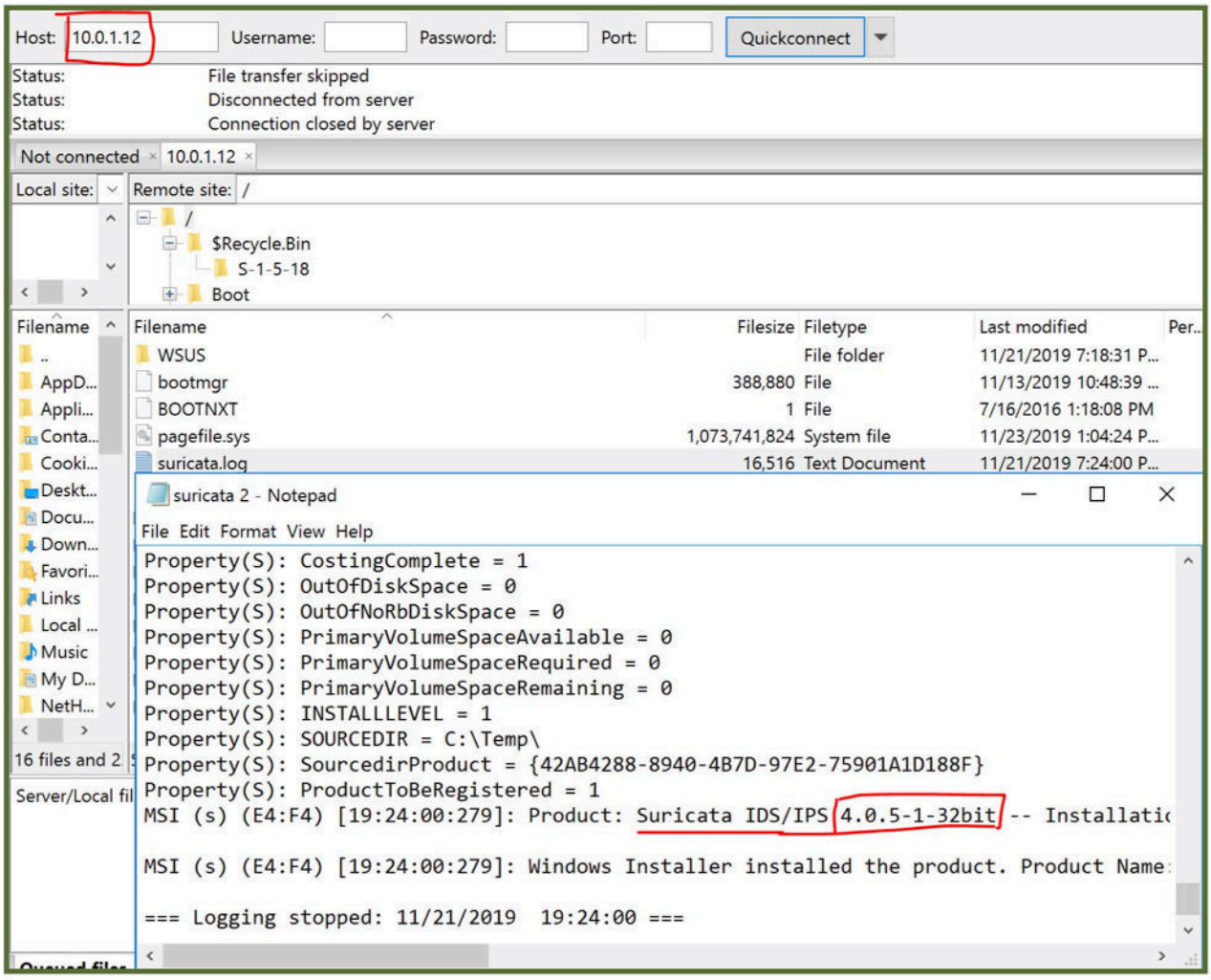
Remediation

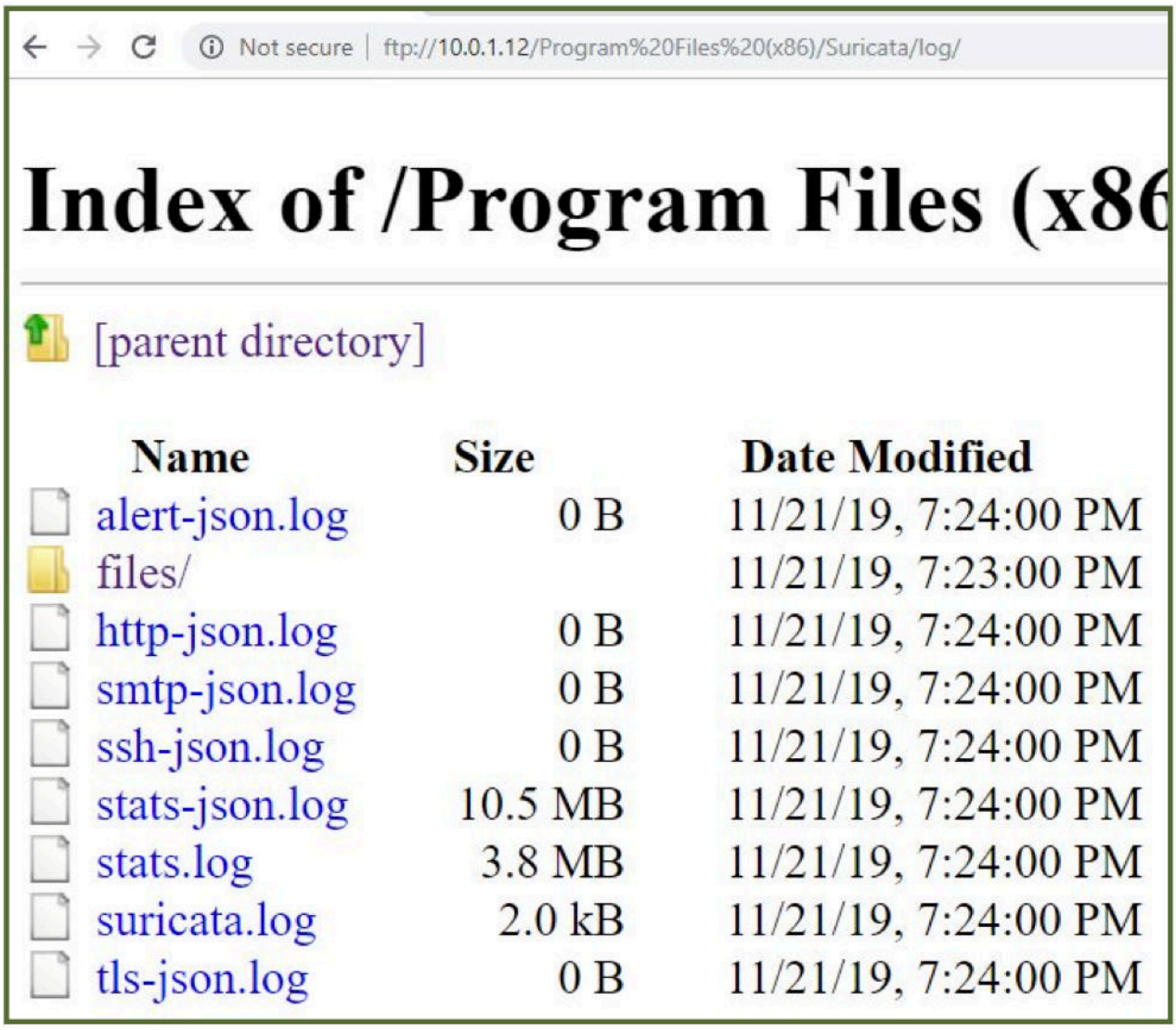
Update Suricata to the latest version 5.0.0.

Assets Affected

- 10.0.1.12 ([redacted]-corp-corp-wsus-01.c.infra-test-environment.internal)

Evidence


Host: 10.0.1.12
Username:
Password:
Port:
Quickconnect
Status: File transfer skipped
Status: Disconnected from server
Status: Connection closed by server
Not connected
10.0.1.12
Local site:
Remote site: /
/
$Recycle.Bin
S-1-5-18
Boot
Filename
Filesize
Filetype
Last modified
WSUS
File folder
11/21/2019 7:18:31 P...
bootmgr
388,880
File
11/13/2019 10:48:39 ...
BOOTNXT
1
File
7/16/2016 1:18:08 PM
pagefile.sys
1,073,741,824
System file
11/23/2019 1:04:24 P...
suricata.log
16,516
Text Document
11/21/2019 7:24:00 P...
suricata 2 - Notepad
File Edit Format View Help
Property(S): CostingComplete = 1
Property(S): OutOfDiskSpace = 0
Property(S): OutOfNoRbDiskSpace = 0
Property(S): PrimaryVolumeSpaceAvailable = 0
Property(S): PrimaryVolumeSpaceRequired = 0
Property(S): PrimaryVolumeSpaceRemaining = 0
Property(S): INSTALLLEVEL = 1
Property(S): SOURCEDIR = C:\Temp\
Property(S): SourcedirProduct = {42AB4288-8940-4B7D-97E2-75901A1D188F}
Property(S): ProductToBeRegistered = 1
MSI (s) (E4:F4) [19:24:00:279]: Product: Suricata IDS/IPS 4.0.5-1-32bit -- Installatic
MSI (s) (E4:F4) [19:24:00:279]: Windows Installer installed the product. Product Name:
=== Logging stopped: 11/21/2019 19:24:00 ===
16 files and 2
Server/Local fil



Suricata Logs found in FTP

Outdated Nginx

An outdated version of Nginx web server was found on the network. This version is vulnerable to exploits that can lead to excessive usage of CPU and memory, as well as an exploit that can crash the worker process or lead to memory disclosure.

Risk Rating

Risk	Impact	Likelihood	Remediation
Medium	Low	High	Low

Infiltration Technique

An https request to the webserver returned a 404 error, the Linux distribution, and Nginx version of the server.

Remediation

Update Nginx to the latest version 1.17.6. Disable additional metadata returned in HTML documents to clients in Nginx.

Assets Affected

- 10.0.2.113 (heads-01.bank.dinobank.us)

Evidence

[redacted]

Unencrypted connection to QueryTree login page

Risk Rating

Risk	Impact	Likelihood	Remediation
Medium	Medium	Medium	Low

Infiltration Technique

Network scanner, with subsequent browsing of the page using.

Remediation

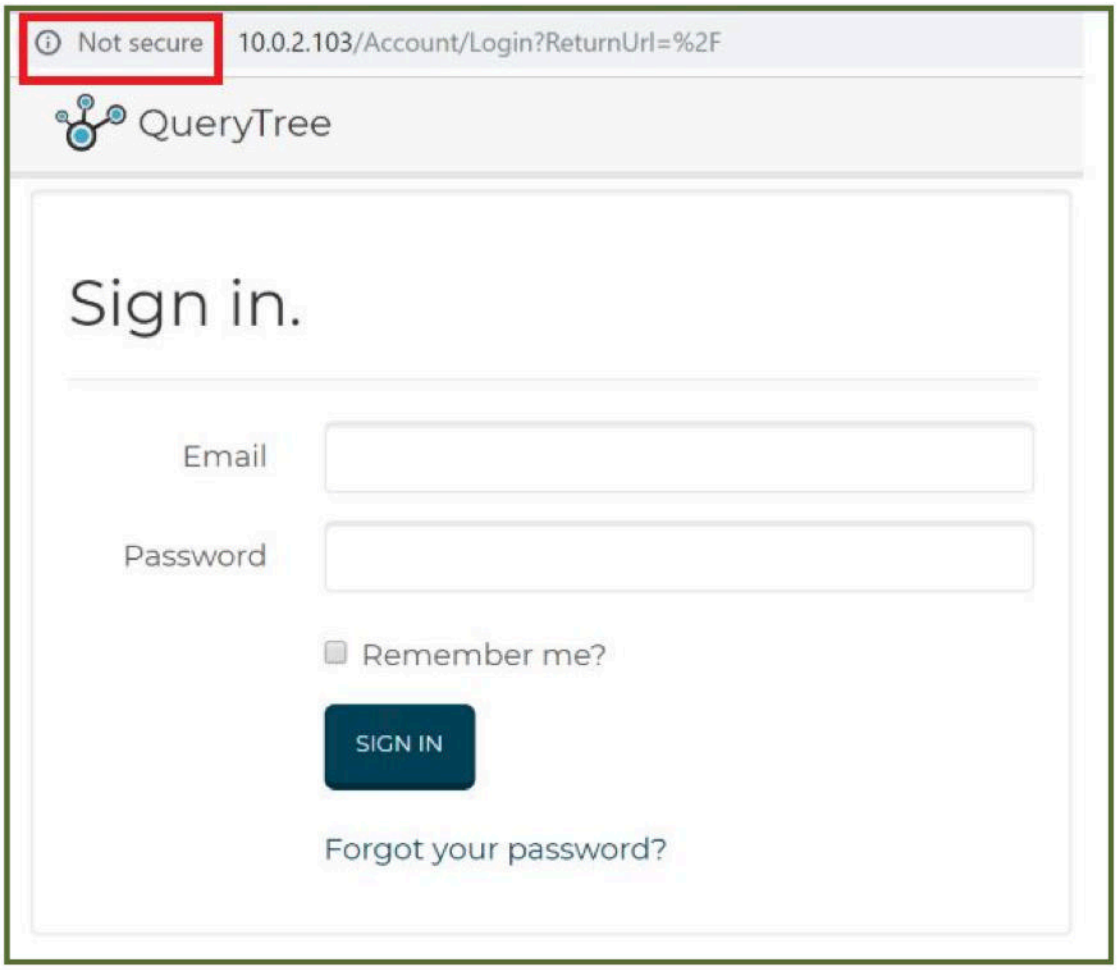
[redacted] suggests implementing SSL/TLS on reports-01.bank.dinobank.us. If properly implemented, the data will be encrypted over SSL/TLS protocol.

As per “NIST Special Publication 800-57 Part 1 Revision 4” Nationals-10 suggests using at least AES-128 for symmetric encryption, and RSA 3072 for asymmetric encryption. Nationals-10 suggests using known libraries like OpenSSL in order to assist with the setup of SSL/TLS on the vulnerable machine.

Assets Affected

- 10.0.2.103 (reports-01.bank.dinobank.us)

Evidence


Not secure
10.0.2.103/Account/Login?ReturnUrl=%2F
QueryTree
Sign in.
Email
Password
Remember me?
SIGN IN
Forgot your password?

Unsecured PostgreSQL database with PII

[redacted] was able to log into the PostgreSQL database on the host 10.0.2.100 using a default username with no password. The database contained PII such as card numbers, card pins, social security numbers, and plaintext passwords alongside the email addresses, names, and addresses. The host is on the Bank network, and the database was used by the bank web interface, ATM, and phone.

[redacted] was able to successfully log in with one of the accounts from the database dump. The team also found a suspicious account with the email address "macgyver@teamblack.co" that had contained one billion dollars, which was also being used by a maintenance contractor at the ATM.

Risk Rating

Risk	Impact	Likelihood	Remediation
Critical	Critical	Critical	Low

Infiltration Technique

During reconnaissance, we discovered the PostgreSQL server in one of our network scans. We attempted to connect to the server using the PostgreSQL client using the username "postgres" (which is a default) with no password, and was successful. We then proceeded to list the databases in the server, and saw the "indominusrex" database, which contained tables such as "accounts", "customers", "employees", and "onlinebanking".

Remediation

We strongly recommend setting a strong password for the "postgres" account. Furthermore, given that it is a default username, you should also consider revoking remote access to that account to reduce the likelihood of brute force attacks. Finally, access to the database server should be restricted to only allow the specific hosts that need it and can be handled by using host-based firewall rules.

Assets Affected

- 10.0.2.100 (core-01.bank.dinobank.us)

Evidence

```
/envs/nationals-cptc [redacted]/kali04 @~ # psql -h 10.0.2.100 -U postgres
psql (12.1 (Debian 12.1-1), server 10.10 (Ubuntu 10.10-0ubuntu0.18.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256,
Type "help" for help.

postgres=# \l
                                    List of databases
     Name      |              Owner               | Encoding | Collate |  Ctyp
---------------+----------------------------------+----------+---------+------
 indominusrex  | a5611a91fc444c1984fa66fe49b226d5 | UTF8     | C.UTF-8 | C.UTF
 postgres      | postgres                         | UTF8     | C.UTF-8 | C.UTF
 template0     | postgres                         | UTF8     | C.UTF-8 | C.UTF
               |                                  |          |         |
 template1     | postgres                         | UTF8     | C.UTF-8 | C.UTF
               |                                  |          |         |
(4 rows)

postgres=# \c indominusrex
psql (12.1 (Debian 12.1-1), server 10.10 (Ubuntu 10.10-0ubuntu0.18.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256,
You are now connected to database "indominusrex" as user "postgres".
indominusrex-# \dt
                 List of relations
 Schema |     Name      | Type  |              Owner
--------+---------------+-------+----------------------------------
 public | accounts      | table | a5611a91fc444c1984fa66fe49b226d5
 public | cds           | table | a5611a91fc444c1984fa66fe49b226d5
 public | customers     | table | a5611a91fc444c1984fa66fe49b226d5
 public | employees     | table | a5611a91fc444c1984fa66fe49b226d5
 public | loans         | table | a5611a91fc444c1984fa66fe49b226d5
 public | onlinebanking | table | a5611a91fc444c1984fa66fe49b226d5
 public | securities    | table | a5611a91fc444c1984fa66fe49b226d5
 public | transactions  | table | a5611a91fc444c1984fa66fe49b226d5
(8 rows)
```

Screenshot showing entry into database server

```
--
-- Data for Name: customers; Type: TABLE DATA; Schema: public; Owner:
a5611a91fc444c1984fa66fe49b226d5
--

COPY public.customers (customerid, taxid, customertype, givenname,
middlename, surname, phonenumber, emailaddr, streetaddr1, streetaddr2,
cityname, statecode, postalcode, companyname, pin, registeredtimestamp)
FROM stdin;
0a804eb8-[redacted]-ba18bf1efd56    [redacted]Retail    Alexander
Bahringer   Russel     +17865303661     alexanderbahringer@gmail.com 3228
Jame Rapids      Metropolis  NY    10103       0000  2019-11-21
17:52:05.879344
49caeef8-[redacted]-fc247967d732    [redacted]Retail    Booker
D     Collier     +16013212521     bookerd@hotmail.com    124 McLaughlin
Centers          Metropolis  NY    10102       0000  2019-11-21
17:52:05.879344
```

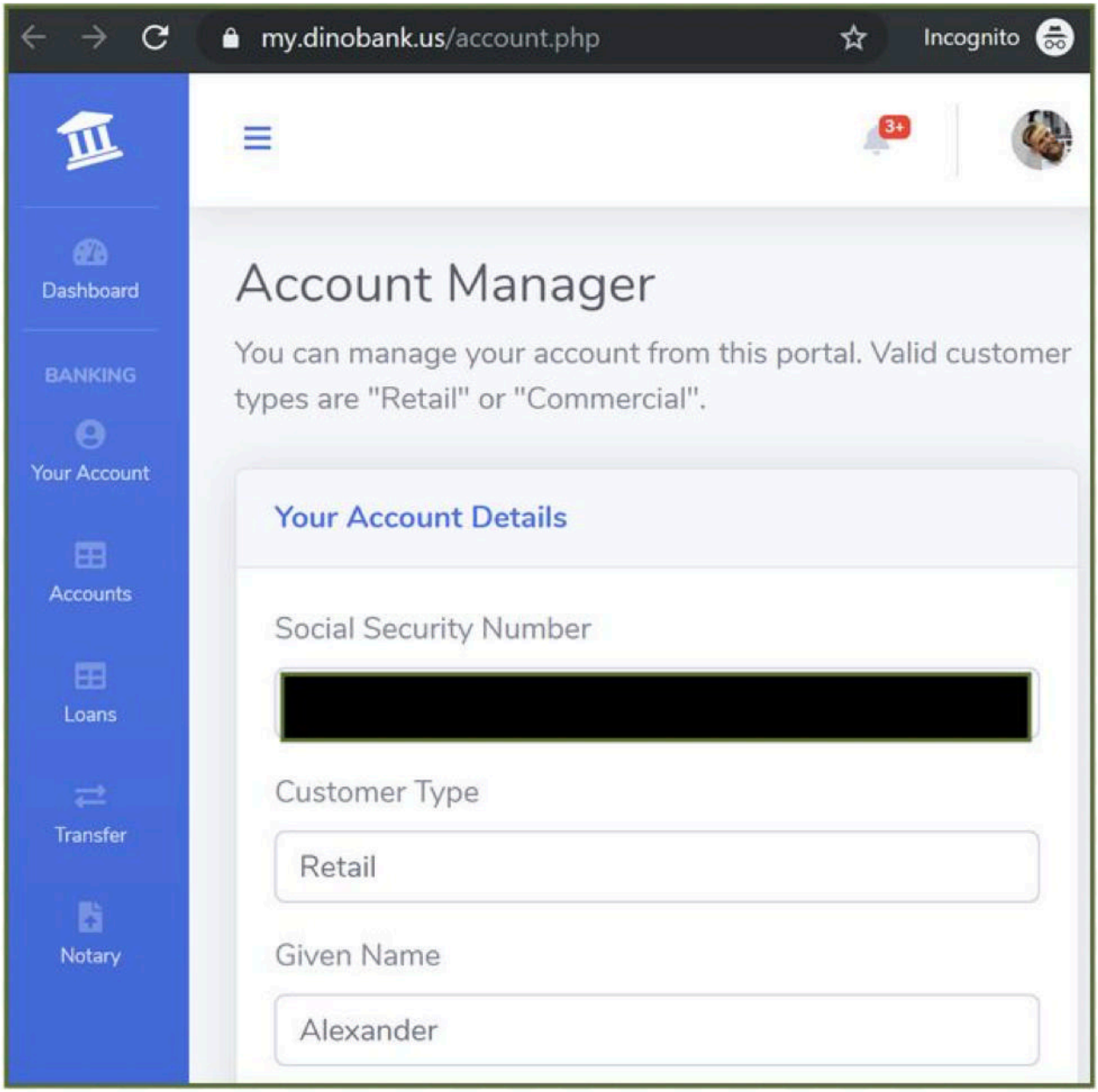
Example data from the customers table

```
--
-- Data for Name: employees; Type: TABLE DATA; Schema: public; Owner:
a5611a91fc444c1984fa66fe49b226d5
--

COPY public.employees (employeeid, loginid, passwd, taxid, givenname,
middlename, surname, phonenumber, emailaddr, streetaddr1, streetaddr2,
cityname, statecode, postalcode, employeetype, title, registeredtimestamp)
FROM stdin;
f650aefa-[redacted]-93a8e04d55ab    Rudy.Beatty@dinobank.us
SbKkDq9S2d [redacted]Rudy  Cartwright  Beatty     +16083376166
Rudy.Beatty@dinobank.us      95486 Berge Views      Metropolis  NY    10106
Manager     Global Consulting Engineer   2019-11-21 17:52:07.035786
```

Example data from the employees table

```
--
-- Data for Name: onlinebanking; Type: TABLE DATA; Schema: public; Owner:
a5611a91fc444c1984fa66fe49b226d5
--

COPY public.onlinebanking (customerid, loginid, passwd) FROM stdin;
0a804eb8-[redacted]-ba18bf1efd56    alexanderbahringer@gmail.com
```

Example data from the onlinebanking table



Screenshot of user's bank web account

Password information on MediaWiki

[redacted] found a wiki page documenting the username format and initial password for employees. Another wiki page listed a password that had previously been used for administrative access and noting that the password had been rotated.

Risk Rating

Risk	Impact	Likelihood	Remediation
Medium	Medium	Medium	Low

Infiltration Technique

After completing network scans and identifying the presence of an HTTP service, we visited the wiki in a web browser. By default, MediaWiki exposes a special page (Special: AllPages) that lists all pages on the wiki, from which we found the pages described above.

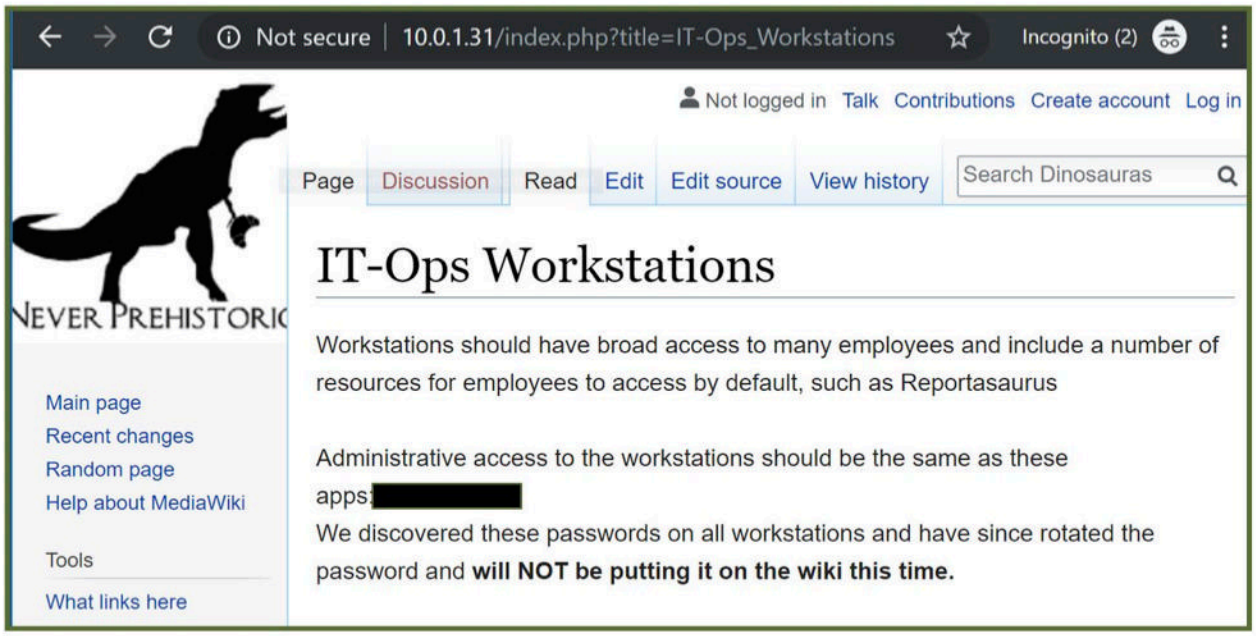
Remediation

The wiki was already using an extension that allows restricting access to pages by user group by adding a small amount of text to the page, as was done on another page on the wiki. However, be aware that the extension is currently listed as unmaintained.

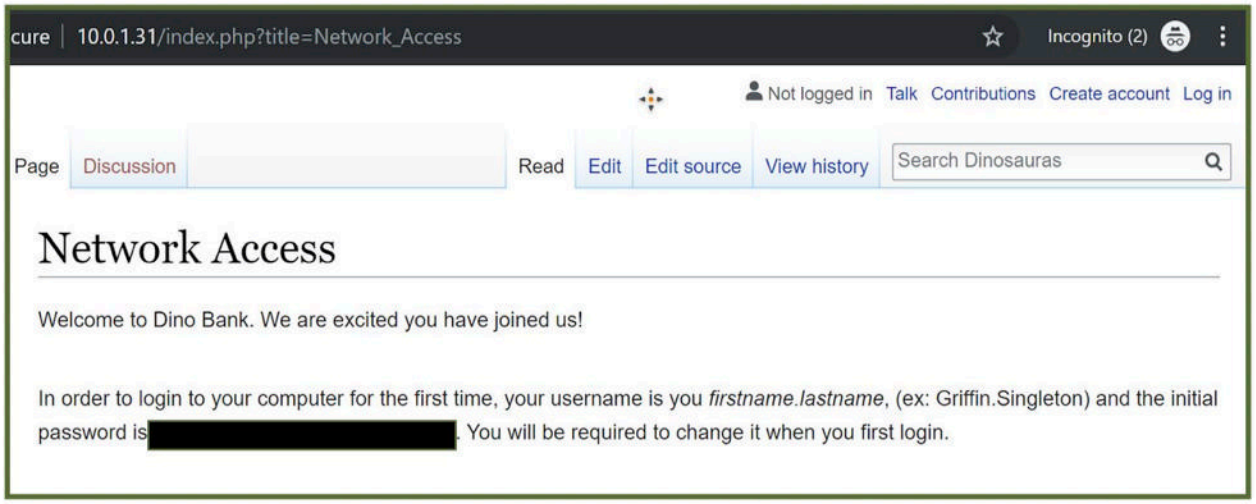
Assets Affected

- 10.0.1.31 ([redacted]-corp-corp-web-01.c.infra-test-environment.internal)

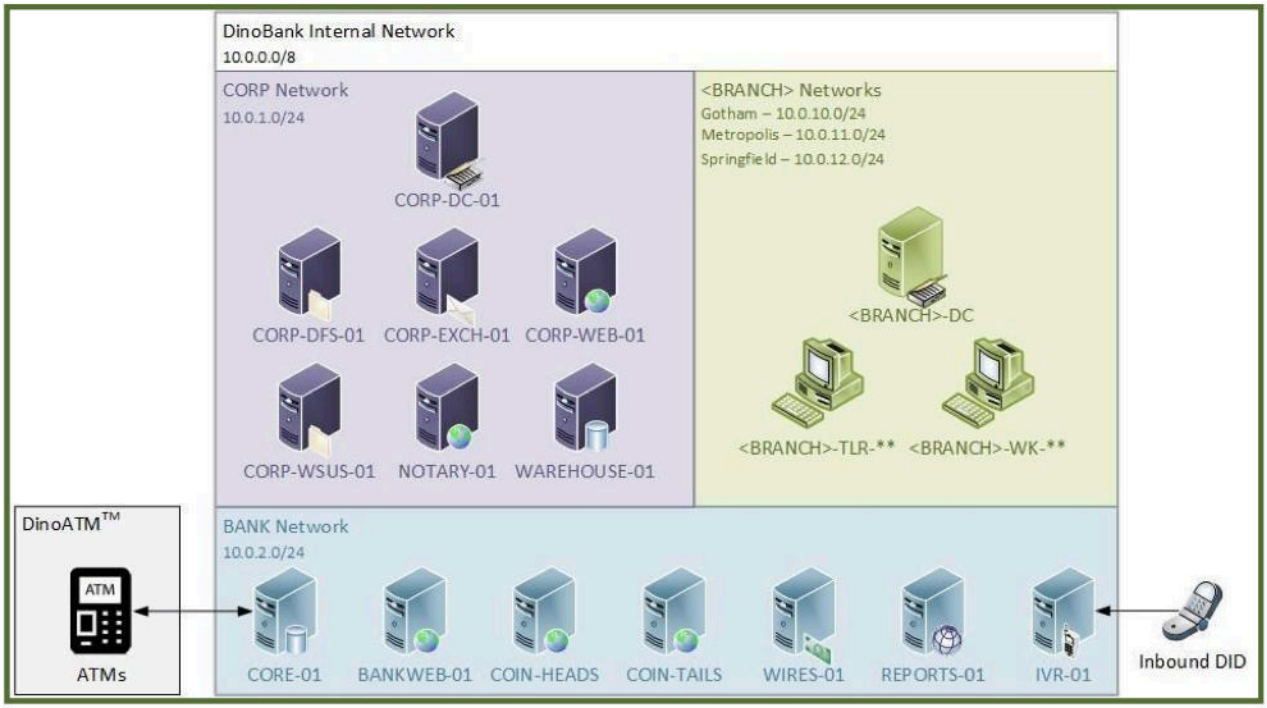
Evidence



WIki page showing previous administrative password for worstations



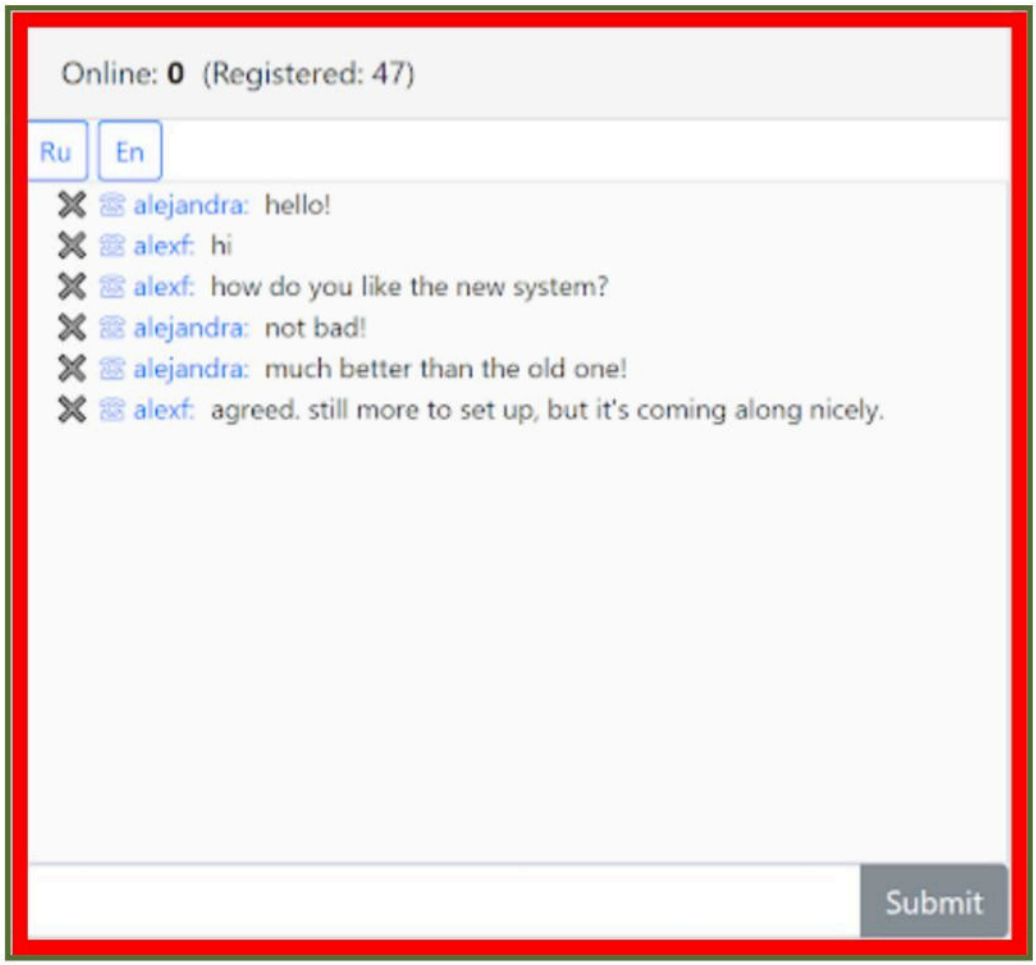
Wiki page showing username and initial password for users



Network diagram found on the wiki

Concerns regarding host “10.0.1.250”

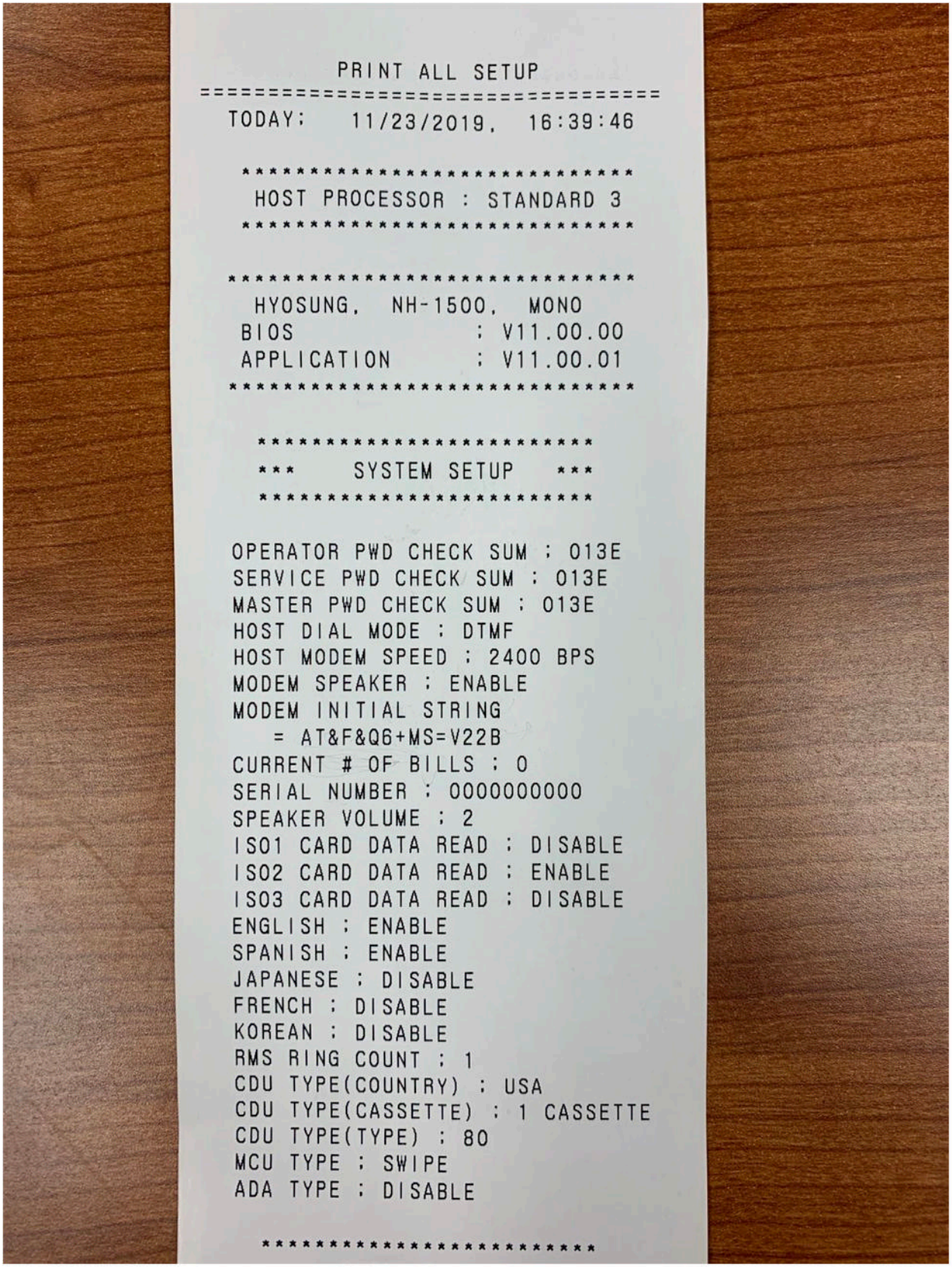
This host in specific has a crypto transaction software called “Open Trade”. The site currently has two users named “alexf” and “alejandra” that are active in the chat.



IVR/ATM Penetration Test Findings

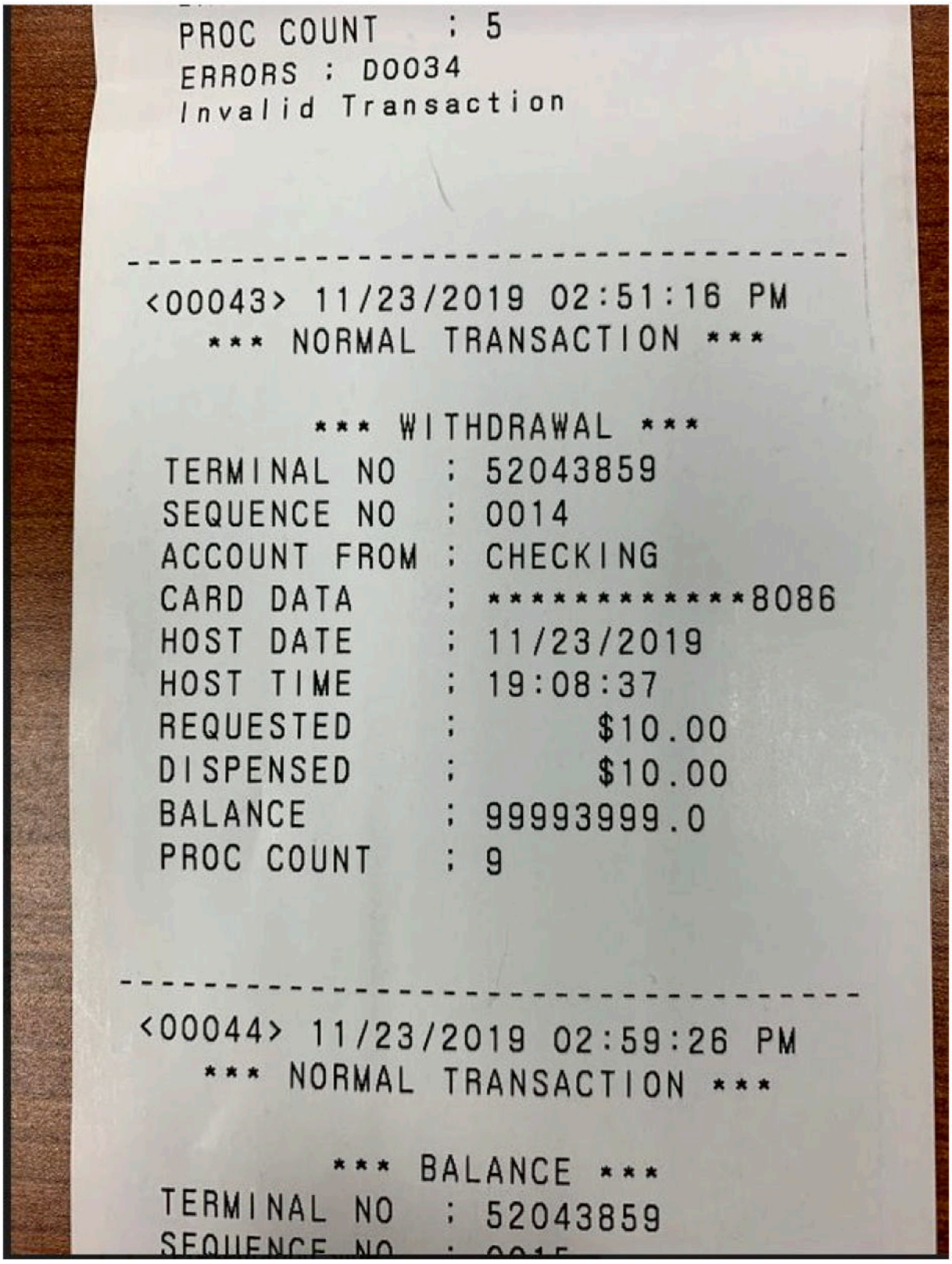
ATM Maintenance Team Neglect

The maintenance team did not conceal sensitive information during the ATM maintenance process. The team was able to shoulder surf and get components of the ATM administrative password. The ATM maintenance team also left the admin configuration screen open without closing it, giving us temporary access to the ATM. With access to the ATM, nationals-10 was able to print out potentially sensitive information from the ATM. Our team also discovered that money was being transferred from an account that contained one billion dollars in it. The ATM was also an outdated model (originally produced in 2004) with a handbook that is easily accessible on the web. Photos of the ATM receipts are provided below (Prior permission was given to take photos).



```
          PRINT ALL SETUP
================================
  TODAY:    11/23/2019,  16:39:46

   ******************************
    HOST PROCESSOR : STANDARD 3
   ******************************

  ******************************
    HYOSUNG,  NH-1500,  MONO
   BIOS              : V11.00.00
   APPLICATION       : V11.00.01
  ******************************

     ************************
     ***    SYSTEM SETUP   ***
     ************************

  OPERATOR PWD CHECK SUM : 013E
  SERVICE PWD CHECK SUM : 013E
  MASTER PWD CHECK SUM : 013E
  HOST DIAL MODE : DTMF
  HOST MODEM SPEED : 2400 BPS
  MODEM SPEAKER : ENABLE
  MODEM INITIAL STRING
     = AT&F&Q6+MS=V22B
  CURRENT # OF BILLS : 0
  SERIAL NUMBER : 0000000000
  SPEAKER VOLUME : 2
  ISO1 CARD DATA READ : DISABLE
  ISO2 CARD DATA READ : ENABLE
  ISO3 CARD DATA READ : DISABLE
  ENGLISH : ENABLE
  SPANISH : ENABLE
  JAPANESE : DISABLE
  FRENCH : DISABLE
  KOREAN : DISABLE
  RMS RING COUNT : 1
  CDU TYPE(COUNTRY) : USA
  CDU TYPE(CASSETTE) : 1 CASSETTE
  CDU TYPE(TYPE) : 80
  MCU TYPE : SWIPE
  ADA TYPE : DISABLE

     ************************
```

[redacted]



```
PROC COUNT    : 5
ERRORS : D0034
Invalid Transaction


-----------------------------------
<00043> 11/23/2019 02:51:16 PM
   *** NORMAL TRANSACTION ***

        *** WITHDRAWAL ***
TERMINAL NO   : 52043859
SEQUENCE NO   : 0014
ACCOUNT FROM  : CHECKING
CARD DATA     : ************8086
HOST DATE     : 11/23/2019
HOST TIME     : 19:08:37
REQUESTED     :       $10.00
DISPENSED     :       $10.00
BALANCE       : 99993999.0
PROC COUNT    : 9


-----------------------------------
<00044> 11/23/2019 02:59:26 PM
   *** NORMAL TRANSACTION ***

        *** BALANCE ***
TERMINAL NO   : 52043859
SEQUENCE NO   : 0015
```

NH-1520 Lookup

IVR Phone (Tax #/SSN and Pin)

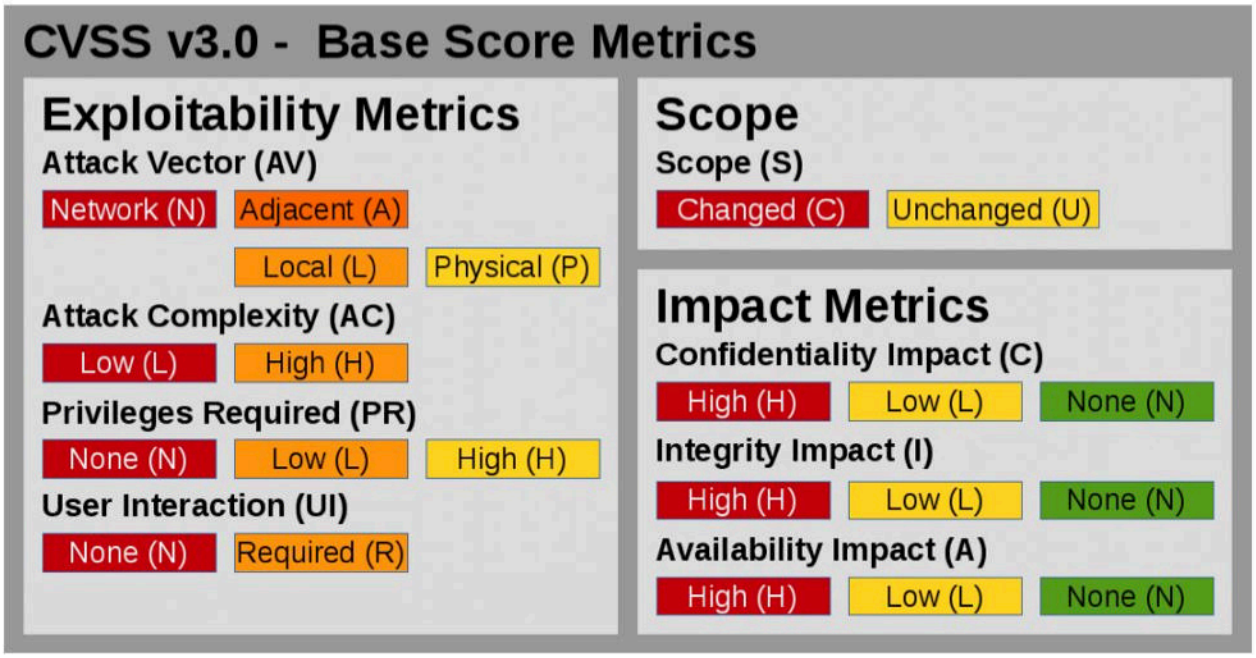
- [redacted] discovered that the IVR system was linked to the same database used for my.dinobank.us website
- The team was able to discover more sensitive information about an account (such as balance) with just a pin number and tax #/social security number.

Vulnerability Scan Analysis

The purpose of this section of the assessment is to identify vulnerabilities within DinoBank's operational environment using automated vulnerability scanning tools such as OpenVas. The output of the vulnerability scan will provide DinoBank with an analysis of vulnerabilities and recommended countermeasures for reducing or mitigating systems' risk of compromise.

Common Vulnerability Scoring System (CVSS)

The common vulnerability scoring system (CVSS) is a vulnerability scoring metrics to capture the characteristics of a vulnerability and provides a numerical score from 1-10 reflecting its severity. The CVSS uses the following metrics below to generate a vulnerability criticality rating.



Vulnerability Scan Summary

Severity	Low	Medium	High	Critical
Vulnerability Count	0	4	0	0

Vulnerable Hosts (Top Five)

IP Address	Vulnerability Count
10.0.1.20	2
10.0.1.12	1
10.0.10.100	1
10.0.10.201	1
10.0.10.202	1

Vulnerable HTTPS Cipher (CVSS 5.0, Medium)

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exist only on HTTPS services.

Vulnerability Detection Result

'Vulnerable' cipher suites accepted by this service via the TLSv1.0, TLSv1.1, TLSv1.2 protocol: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
Ports: 443, 444

Solution (Mitigation)

The configuration of these services should be changed so that it does not accept the listed cipher suites anymore.

Affected Machines

10.0.1.20	[redacted]-corp-corp-exch-01.c.infra-test-environment.internal

Unencrypted FTP Login (CVSS 4.8, Medium)

Summary

The remote host is running an FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Anonymous sessions: 331 Password required for anonymous
Non-anonymous sessions: 331 Password required for openvas-vt

Solution (Mitigation)

Enable FTPS or enforce the connection via the 'AUTH TLS' command.

Affected Machines

10.0.1.12	[redacted]-corp-corp-wsus-01.c.infra-test-environment.internal

Weak Cipher Suites (CVSS 4.3, Medium)

Summary

Remote Desktop connection service accepts weak SSL/TLS cipher suites.

Vulnerability Detection Result

'Weak' cipher suites accepted by this service via the TLSv1.0, TLSv1.1, TLSv1.2 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

Solution (Mitigation)

The configuration of these services should be changed so that it does not accept the listed weak cipher suites anymore.

Affected Machines

10.0.10.100	[redacted]-branch-gotham-gotham-dc.c.infra-test-environment.internal
10.0.10.201	[redacted]-branch-gotham-gotham-tlr-01.c.infra-test-environment.internal
10.0.10.202	[redacted]-branch-gotham-gotham-tlr-02.c.infra-test-environment.internal
10.0.10.203	[redacted]-branch-gotham-gotham-tlr-03.c.infra-test-environment.internal
10.0.10.208	[redacted]-branch-gotham-gotham-wk-01.c.infra-test-environment.internal
10.0.10.209	[redacted]-branch-gotham-gotham-wk-02.c.infra-test-environment.internal
10.0.11.100	[redacted]-branch-metro-metro-dc.c.infra-test-environment.internal
10.0.11.201	[redacted]-branch-metro-metro-tlr-01.c.infra-test-environment.internal
10.0.11.202	[redacted]-branch-metro-metro-tlr-02.c.infra-test-environment.internal
10.0.11.208	[redacted]-branch-metro-metro-wk-01.c.infra-test-environment.internal
10.0.12.201	[redacted]-branch-spring-spring-tlr-01.c.infra-test-environment.internal
10.0.12.208	[redacted]-branch-spring-spring-wk-01.c.infra-test-environment.internal

Weak Signature Algorithm (CVSS 4.0, Medium)

Summary

The remote service is using an SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

The following certificates are part of the certificate chain but using insecure signature algorithms:

Subject: CN=corp-exch-01
Signature Algorithm: sha1WithRSAEncryption
Ports: 2525, 587, 465, 444, 443, 25

Solution (Mitigation)

Servers that use outdated SSL/TLS hashing algorithms should upgrade to at least SHA-2 hashing algorithm

Affected Machines

10.0.1.20	[redacted]-branch-gotham-gotham-dc.c.infra-test-environment.internal

Open Source Intelligence Gathering (OSINT)

The Open Source Intelligence Gathering (OSINT) portion of the assessment is a service that [redacted] provides as part of the reconnaissance phase of our penetration test. The OSINT assessment refers to all unclassified information and includes anything freely available on the Web. As part of this test, [redacted] attempted to retrieve open source information regarding DinoBank.

During the assessment, many tools were used to enumerate through domains and find subdomains, and trace activity with individual names over social media sites. Most of this was secure and posed no threat. Using Prowl, a script to enumerate through a company's LinkedIn profile and intensify listed employees and possible email accounts using the standard naming scheme. (shown below)

Dino	Dedić	dino.dedi@dinobank.us
Ruth	Brooks	ruth.brooks@dinobank.us
Lokesh	Pandey	lokesh.pandey@dinobank.us
Joshua	Jones	joshua.jones@dinobank.us
Nick	DiMaggio	nick.dimaggio@dinobank.us
Lawrence	Hayden	lawrence.hayden@dinobank.us
Brad	Alleman	brad.alleman@dinobank.us
John[redacted]	Gay	johnathan.gay@dinobank.us
Margus[redacted]	Slaughter	margus.slaughter@dinobank.us
Luis	Garduno	luis.garduno@dinobank.us
Jacqueline	Woods	jacqueline.woods@dinobank.us
Samara	Romero	samara.romero@dinobank.us
Travistene	Jones	travistene.jones@dinobank.us
Rebecca	Stiegler	rebecca.stiegler@dinobank.us
Kennan	Wright	kennan.wright@dinobank.us
Dahlia	Dawson	dahlia.dawson@dinobank.us
Dan	Oliver	dan.oliver@dinobank.us
Ariel	Robinson	ariel.robinson@dinobank.us
Jamie	Davenport	jamie.davenport@dinobank.us
Paul	Alvarado	paul.alvarado@dinobank.us
Alex	Faulkner	alex.faulkner@dinobank.us
Tom	Dickson	tom.dickson@dinobank.us
Precious	Braun	precious.braun@dinobank.us
Mitchell	Zamora	mitchell.zamora@dinobank.us
Heather	Potter	heather.potter@dinobank.us
Mckayla	Pearson	mckayla.pearson@dinobank.us
isaiah	grimes	isaiah.grimes@dinobank.us
Peter	Aline	peter.aline@dinobank.us

The other information found on the web regarding DinoBank was a server record on Shodan (an IoT search engine) for an exposed Postfix server. These in themselves may not be a threat, but the possibility of leveraging this information in an attack could be drastic. (search results below)


```
220 dinobank-us-public-mx.c.infra-test-environment.internal ESMTP Postfix (Debian/GNU)
250-dinobank-us-public-mx.c.infra-test-environment.internal
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
```

As DinoBank grows its online presence, more information will be available online. Because of this, as DinoBank grows, it must be ensured that no sensitive information is publically available and that there are no clues to internal credentials online.

Recommendations

Plan of Action and Milestones

[redacted] has provided an overall strategic roadmap intended to provide a timeline for the remediation strategies outlined in the technical analysis and appendices. While the final decision on how to respond to the vulnerabilities shown in the report is dependent on DinoBank. The following plan of action will help increase DinoBank's cybersecurity maturity level.

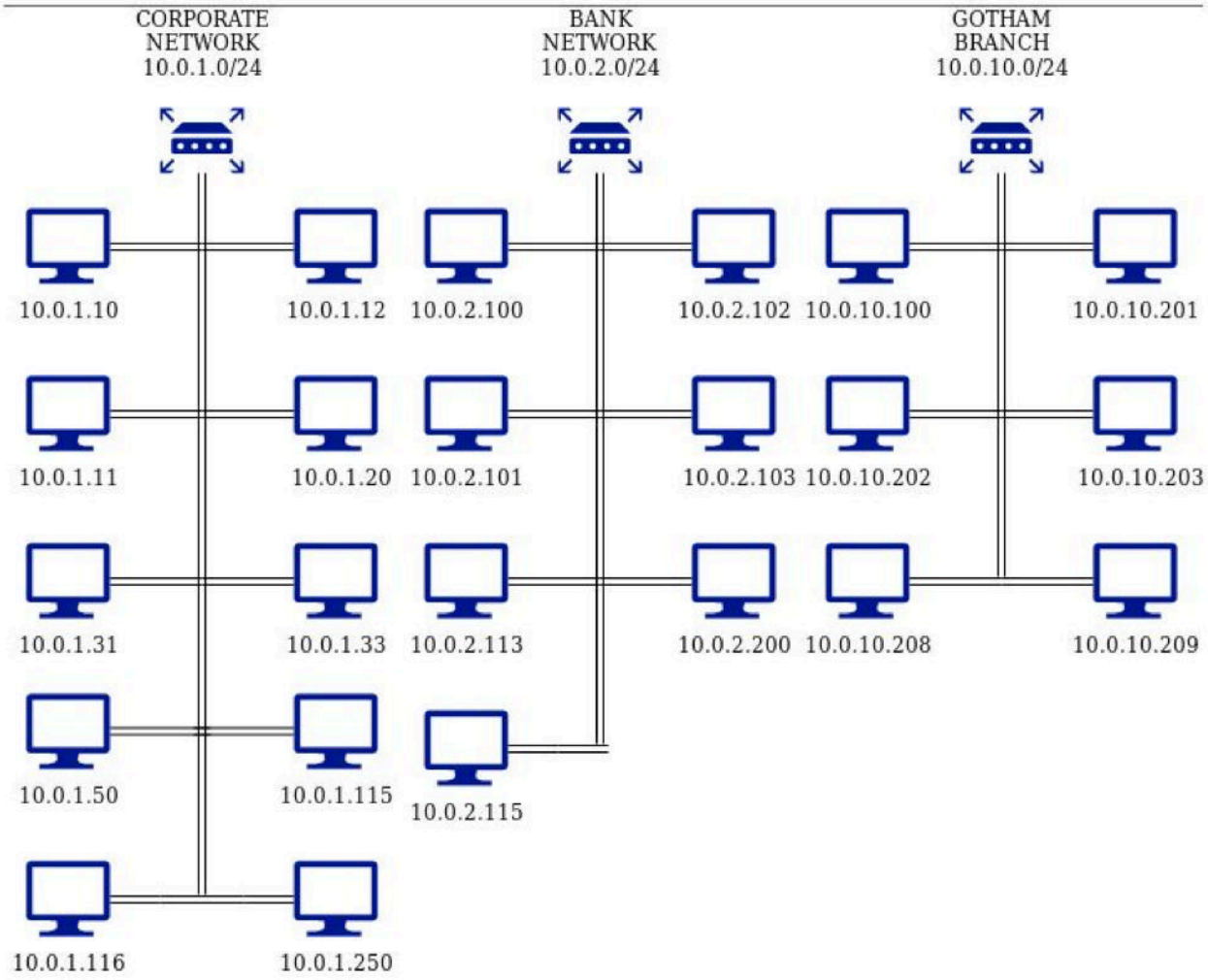
Action Plan

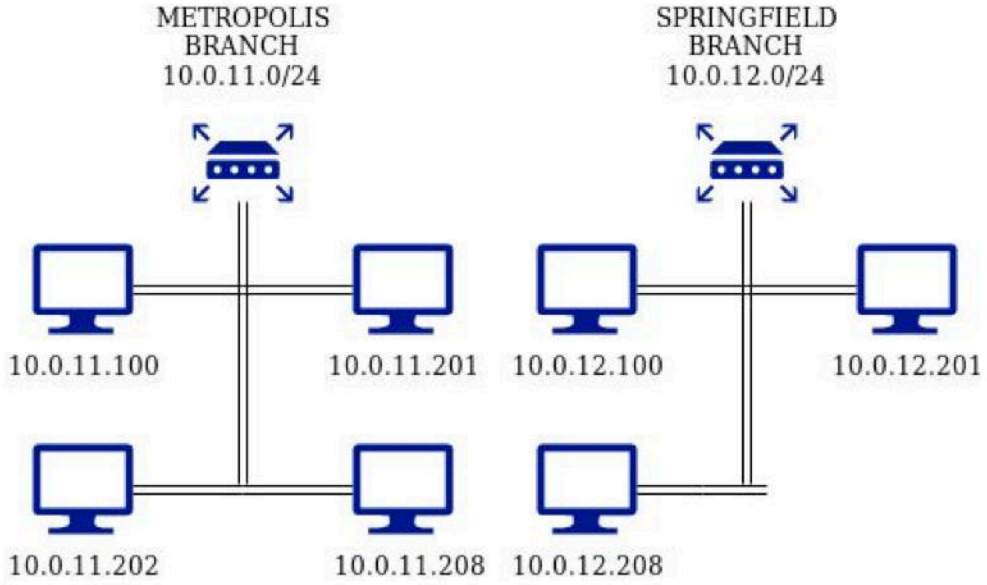
ID	Immediately
1.0	Define a project lead for initializing the action plan
1.1	Patch outdated services and remove unused/deprecated services
1.2	Implement passwords across all systems in accordance with the corporate password policy
ID	**One Month**
2.0	Identify any possible discrepancies with the report and work with [redacted] to resolve any concerns
2.1	Analyze risk and vulnerabilities • Align internal cyber risk structure with the risk outlined in this report • Identify the most critical risks and complete mitigation
ID	**Two to Six Months**
3.0	Full user account and user privilege audit (Domain Controller Audit)
3.1	Assemble security task force to maintain DinoBank internal security controls
3.2	Rescan DinoBank's corporate network to validate remediation efforts
ID	**Six Months to One Year**
4.0	Review network layout and implement segmentation

ID	After One Year
5.0	Conduct an annual penetration assessment to maintain DinoBank's security posture

Appendices

Appendix 1: Network Topology




METROPOLIS
BRANCH
10.0.11.0/24
SPRINGFIELD
BRANCH
10.0.12.0/24
10.0.11.100
10.0.11.201
10.0.12.100
10.0.12.201
10.0.11.202
10.0.11.208
10.0.12.208

Appendix 2: TCP Network Scan Results

IP / HOSTNAME	Port:Service
SUBNET 10.0.1.0/24	
10.0.1.10 [redacted]-corp-corp-dc-01.c.infra-test-environment.internal	53:domain 88:kerberos-sec 135:msrpc 139:netbios-ssn 389:ldap 445:microsoft-ds 464:kpasswd5 593:ncacn_http 636:tcpwrapped 3268:ldap 3269:tcpwrapped 3389:ms-wbt-server 5985:http 5986:http 9389:mc-nmf 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49669:msrpc 49671:ncacn_http 49672:msrpc 49674:msrpc 49683:msrpc 49699:msrpc 61554:msrpc
10.0.1.11 [redacted]-corp-corp-dfs-01.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49669:msrpc 49673:msrpc

	49675:msrpc 49678:msrpc
10.0.1.12 [redacted]corp-wsus-01.c.infra-test-environment.internal	21:ftp 80:http 135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 8530:http 8531:unknown 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49670:msrpc 49674:msrpc 49676:msrpc 49678:msrpc
10.0.1.20 [redacted]-corp-exch-01.c.infra-test-environment.internal	25:smtp 80:http 81:http 135:msrpc 139:netbios-ssn 443:http 444:http 445:microsoft-ds 465:smtp 475:smtp 476:smtp 477:smtp 587:smtp 593:ncacn_http 717:smtp 808:ccproxy-http 890:mc-nmf 1801:msmq 2103:msrpc 2105:msrpc 2107:msrpc 2525:smtp 3389:ms-wbt-server 3800:http 3801:mc-nmf 3803:mc-nmf 3823:mc-nmf

	3828:mc-nmf 3843:mc-nmf 3863:mc-nmf 3867:mc-nmf 3875:msexchange-logcopier 5060:sip 5062:na-localise 5065:ca-2 5985:http 5986:http 6001:ncacn_http 6014:msrpc 6088:msrpc 6131:msrpc 6149:msrpc 6159:msrpc 6163:msrpc 6167:msrpc 6172:msrpc 6178:msrpc 6179:msrpc 6183:msrpc 6187:msrpc 6188:msrpc 6189:msrpc 6191:msrpc 6192:msrpc 6193:msrpc 6194:msrpc 6203:msrpc 6207:msrpc 6220:msrpc 6245:msrpc 6283:msrpc 6296:msrpc 6310:msrpc 6314:msrpc 6323:msrpc 6377:msrpc 6400:msrpc 6401:msrpc 6402:msrpc 6403:msrpc 6404:msrpc 6410:msrpc 6411:msrpc 6437:msrpc 6441:msrpc 6458:msrpc

	6528:msrpc 6554:msrpc 6588:msrpc 6607:msrpc 6646:msrpc 6667:msrpc 6688:msrpc 6710:msrpc 6773:msrpc 7065:msrpc 8172:http 9710:mc-nmf 41301: 47001:http 64327:msexchange-logcopier 64337:mc-nmf
10.0.1.31 [redacted]-corp-corp-web-01.c.infra-test-environment.internal	80:http 135:msrpc 139:netbios-ssn 445:microsoft-ds 3306:mysql 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49668:msrpc 49675:msrpc 49677:msrpc 49678:msrpc
10.0.1.33 [redacted]-corp-corp-web-03.c.infra-test-environment.internal	22:ssh 80:http 443:http
10.0.1.50 [redacted]-corp-warehouse.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49669:msrpc 49672:msrpc

	49675:msrpc 49676:msrpc
10.0.1.115 [redacted]-corp-corp-jgay-ws.c.infra-test-environment.internal	3389:ms-wbt-server 5986:http
10.0.1.116 nationals-t10-corp-corp-tdickson-ws.c.infra-test-environment.internal	3389:ms-wbt-server 5986:http
10.0.1.250 [redacted]-corp-coins-01.c.infra-test-environment.internal	22:ssh 80:http 443:http 40545:tcpwrapped 40745:http
SUBNET 10.0.2.0/24	
10.0.2.100 core-01.bank.dinobank.us	22:ssh 80:http 443:http 5432:postgresql 9001:tor-orport
10.0.2.101 bankweb-01.bank.dinobank.us	22:ssh 80:http 443:http
10.0.2.102 ivr-01.bank.dinobank.us	22:ssh 5038:asterisk
10.0.2.103 reports-01.bank.dinobank.us	22:ssh 80:tcpwrapped
10.0.2.113 heads-01.bank.dinobank.us	22:ssh 80:http 443:http
10.0.2.115 tails-01.bank.dinobank.us	22:ssh 80:http 443:http 8000:http
10.0.2.200 wires-01.bank.dinobank.us	22:ssh
SUBNET 10.0.10.0/24	
10.0.10.100 [redacted]-branch-gotham-gotham-dc.c.infra-test-environment.internal	53:domain 88:kerberos-sec 135:msrpc 139:netbios-ssn 389:ldap 445:microsoft-ds 464:kpasswd5 593:ncacn_http 636:tcpwrapped

	3268:ldap 3269:tcpwrapped 3389:ms-wbt-server 5985:http 5986:http 9389:mc-nmf 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49668:msrpc 49671:msrpc 49677:ncacn_http 49678:msrpc 49680:msrpc 49688:msrpc 61323:msrpc 62669:msrpc
10.0.10.201 [redacted]-branch-gotham-gotham-tlr-01.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49672:msrpc 49674:msrpc 49676:msrpc 49681:msrpc
10.0.10.202 [redacted]-branch-gotham-gotham-tlr-02.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49670:msrpc 49674:msrpc 49676:msrpc 49681:msrpc

10.0.10.203 [redacted]-branch-gotham-gotham-tlr-03.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49670:msrpc 49673:msrpc 49680:msrpc 49681:msrpc
10.0.10.208 [redacted]-branch-gotham-gotham-wk-01.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49669:msrpc 49674:msrpc 49676:msrpc 49677:msrpc
10.0.10.209 [redacted]-branch-gotham-gotham-wk-02.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49671:msrpc 49674:msrpc 49677:msrpc 49681:msrpc
SUBNET 10.0.11.0/24	

10.0.11.100 [redacted]-branch-metro-metro-dc.c.infra-test-environment.internal	53:domain 88:kerberos-sec 135:msrpc 139:netbios-ssn 389:ldap 445:microsoft-ds 464:kpasswd5 593:ncacn_http 636:tcpwrapped 3268:ldap 3269:tcpwrapped 3389:ms-wbt-server 5985:http 5986:http 9389:mc-nmf 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49668:msrpc 49671:msrpc 49675:ncacn_http 49676:msrpc 49678:msrpc 49686:msrpc 49733:msrpc 63738:msrpc
10.0.11.201 [redacted]-branch-metro-metro-tlr-01.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49673:msrpc 49674:msrpc 49676:msrpc 49681:msrpc
10.0.11.202 [redacted]-branch-metro-metro-tlr-02.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http

	47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49670:msrpc 49675:msrpc 49676:msrpc 49681:msrpc
10.0.11.208 [redacted]-branch-metro-metro-wk-01.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49669:msrpc 49674:msrpc 49676:msrpc 49677:msrpc
SUBNET 10.0.12.0/24	
10.0.12.100 [redacted]-branch-spring-spring-dc.c.infra-test-environment.internal	53:domain 88:kerberos-sec 135:msrpc 139:netbios-ssn 389:ldap 445:microsoft-ds 464:kpasswd5 593:ncacn_http 636:tcpwrapped 3268:ldap 3269:tcpwrapped 3389:ms-wbt-server 5985:http 5986:http 9389:mc-nmf 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49671:msrpc 49675:ncacn_http

	49676:msrpc 49678:msrpc 49687:msrpc 49720:msrpc 61095:msrpc
10.0.12.201 [redacted]-branch-spring-spring-tlr-01.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49670:msrpc 49675:msrpc 49680:msrpc 49681:msrpc
10.0.12.208 [redacted]-branch-spring-spring-wk-01.c.infra-test-environment.internal	135:msrpc 139:netbios-ssn 445:microsoft-ds 3389:ms-wbt-server 5985:http 5986:http 47001:http 49664:msrpc 49665:msrpc 49666:msrpc 49667:msrpc 49670:msrpc 49674:msrpc 49676:msrpc 49681:msrpc