A black and white logo

Description automatically generated

**Metropolis Transit corporation**

**Risk Assessment Report.**

Document Tracking

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Version** | **Date of Version** | **Author responsible for the change** | **Brief Explanation of the change** |
| 1.0 | 11/13/2023 | Leen Abdallah | First Draft |
| 2.0 | 11/14/2023 | Malek Salem | Minor change in the table of content |
| 3.0 | 11/16/2023 | Ahmad al Sayeh | Update on the Attack graph |
| 4.0 | 11/19/2023 | Leen abdallah | Final check |

Contents

[Executive Summary 3](#_Toc151247477)

[System Overview 4](#_Toc151247478)

[DMZ Network Overview. 4](#_Toc151247479)

[Technology Information System -TIS Subnet- 5](#_Toc151247480)

[Enterprise Subnet 5](#_Toc151247481)

[Garbage Subnet 5](#_Toc151247482)

[System Decomposition 6](#_Toc151247483)

[Adversary Analysis 7](#_Toc151247484)

# Executive Summary

As a starting point in order to deeply understand the system we created [threat library](Threat_Library.xlsx) that represents all of the threats in the system as well as the same applies to the [vulnerabilities](Vulnerability_Library.xlsx), in which each vulnerability or entry point that might be exploited by an attacker could be linked with more than one threat.

Then we focus on the OS’s that our servers runs on, some of them we’re obsolete and requires patch management and applying updates to in order to avoid any flaws that they represent some of them run on windows OS such as the Active Directory where all the credentials are hosted, runs on windows 2012 which introduces zero logon vulnerability that can be cascaded into severe attacks that majorly affect the organization financially and reputational wise, for each vulnerability we linked it with [STRIDE](STRIDE.xlsx) framework to see how it affects Metropolis, does it spoof on the users identity or cause degradation in the service and recommend some [controls and mitigations](STRIDE.xlsx) that we apply for metropolis and it’s their decision to whether consider it or not.

Then we linked between Assets, threats, and vulnerabilities by using [TVA spreadsheet](TVA.xlsx) to assess the risk by representing each asset vulnerable to the threat that might exploit the vulnerability.

Finally, in order to prioritize the point that we have to start the fix by we assess the risk by measuring likelihood of occurrence, value of the asset based on the organization operations that is linked with and we used quantitively based [risk assessment](RISK%20ASSESSMENT.xlsx) using equation that measures the risk by multiplying the asset value with likelihood adding any uncertainty minus the controls that might reduce the impact of the exposure and check if there are any available controls.

Then the process will finally focus on checking if the risk associated is above the risk tolerance which means that the organization can handle it or not, which the organization risk tolerance was acceptable for any value that is below 4 otherwise it represents risk to the organization and needs to be handled immediately, beside in order to understand how the attacker can exploit the Vulnerability we represent the major risk using attack Graphs.

* <Zerologon.drawio.png>
* <Lack_of_UEBA.drawio.png>

# System Overview

## DMZ Network Overview.

|  |  |
| --- | --- |
| router1.metropolistransit.net | This system serves as a router with the IP addresses 192.168.207.1 and 10.1.0.1. It runs pfSense as its operating system and provides external services such as HTTP, HTTPS, and SSH, but these services are accessible only from the LAN, not the WAN. |
| ns1.metropolistransit.net | Operating on IP addresses 192.168.207.2 and 10.1.0.2, this Windows 2016 system functions as a DNS server. External access is allowed, but certain services like NetBios and SMB are blocked at the firewall. |
| ns2.metropolistransit.net | Like ns1, ns2.metropolistransit.net is a Windows 2016 DNS server with IP addresses 192.168.207.3 and 10.1.0.3. It also blocks NetBios and SMB at the firewall. |
| www.metropolistransit.net | Running Ubuntu 16.04 with IP addresses 192.168.207.4 and 10.1.0.4, this system provides external services including HTTP, HTTPS, and SSH (limited to 10.1.0.0). |
| mail.metropolistransit.net | This Ubuntu 16.04 system (IP addresses 192.168.207.5 and 10.1.0.5) serves as a mail server, offering SMTP, IMAP, POP3, HTTP, and HTTPS services. SSH access is restricted to the 10.1.0.0 network. |
| ftp.metropolistransit.net | Operating on Ubuntu 16.04 with IP addresses 192.168.207.6 and 10.1.0.6, this system functions as an FTP server, and it allows SSH access from the 10.1.0.0 network. |
| www2.metropolistransit.net | Like www.metropolistransit.net, this Ubuntu 16.04 system (IP addresses 192.168.207.7 and 10.1.0.7) provides HTTP/HTTPS services and SSH access limited to the 10.1.0.0 network. |
| api.metropolistransit.net | Running Ubuntu 14.04 with IP addresses 192.168.207.8 and 10.1.0.8, this system offers HTTPS services and allows SSH access from the 10.1.0.0 network. |
| sftp.metropolistransit.net | This Ubuntu 16.04 system (IP addresses 192.168.207.9 and 10.1.0.9) serves as an SFTP server, providing secure file transfer services. SSH access is limited to the 10.1.0.0 network. |
| DataBase -db- | Operating on IP address 10.1.0.10, this Ubuntu 16.04 system functions as a MySQL server, with SSH access restricted to the 10.1.0.0 network. |
| router2 | This system with the IP address 10.1.255.1 serves as a router but is not Internet accessible. |
| ceo.metropolistransit.net | Operating on IP addresses 192.168.207.10, 10.1.255.2, and 192.168.1.3, this Windows 10 system serves as the CEO's system and allows Remote Desktop Protocol (RDP) access. |
| <All IoT devices> | These Ubuntu 14.04 devices with IP addresses ranging from 10.1.10.1 to 10.1.10.200 are not Internet accessible and serve as IoT devices with SSH access. |

## Technology Information System -TIS Subnet-

|  |  |
| --- | --- |
| router2.metropolistransit.net | This system operates as a router using pfSense as its operating system. It provides external services such as SSH, HTTP, HTTPS, and DNS. |
| ad.metropolistransit.net | This system, running Windows 2012 Standard, functions as an Active Directory (AD) server, providing standard AD services for the network. |
| siem.metropolistransit.net | Operating on the OSSIM platform (Open-Source Security Information Management), this system offers standard services for security information management. |
| warehouse.metropolistransit.net | This Ubuntu 12.04 system functions as a warehouse server, providing services such as SSH for secure shell access and MySQL for database management. |

## Enterprise Subnet

|  |  |
| --- | --- |
| router2.metropolistransit.net | This system operates as a router with the IP address 192.168.1.1, running pfSense as its operating system. It provides services such as SSH, HTTP, HTTPS, and DNS. |
| <lname>.metropolistransit.net | This system, dynamically assigned within the DHCP range 192.168.1.10-255, operates on the Windows 10 operating system. It provides standard Windows services and functionalities. Please replace "<lname>" with the specific name or label for this system. |

## Garbage Subnet

|  |  |
| --- | --- |
| router2.metropolistransit.net | This system operates as a router with the IP address 192.168.2.1, running pfSense as its operating system. It provides services such as SSH, HTTP, HTTPS, and DNS. |
| <assorted> | Description: This system, dynamically assigned within the DHCP range 192.168.2.10-255, has an assorted configuration with various instances running Windows XP SP0-3 and Windows 7. It provides standard Windows services and functionalities. Please replace "<assorted>" with a specific name or label for this system. |

# 

# System Decomposition

To better understand the system, we decompose it to be able to know entry points and exit ones, we focus on the assets the help by performing the organization operations.

Such as the IoT devices they are entry points where the users interact with the system to purchase a ticket from metropolis transit online that could pose a risk to the organization if there is lack of UEBA, as well as the exit points such as web servers and routers that they deliver response to the users they could be using obsolete OS and put the organization at risk, for [more details](Risk%20Management.xlsx).

# 

# Adversary Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Adversary Analysis Frameworks | Coordinated Insider Attacks | Ransomware Attack | Reputational Damage | Unauthorized Access |
| Motivation | Financial Gain, Revenge | Financial Gain | Competitive Advantage | Financial Gain |
| Ideology | Hacktivist Insiders | Extortionists | Activist Groups | Hacktivists |
| Coercion | Nation-States or External Threat Actors | State-Sponsored Actors | Competitors or Extortionists | Nation-States or External Threat Actors |
| Ego | Competitive Espionage | Hacktivist Groups | Individuals Seeking Recognition | Competitive Espionage |
| Revenge | Disgruntled Employees | Disgruntled Insiders | Disgruntled Insiders | Disgruntled Insiders |
| Ambition | Competing Companies | Competing Criminal Organizations | Competing Companies | Competing Companies |
| Sabotage | Nation-States | Nation-States | Nation-States | Nation-States |
| Criminal Intent | Organized Crime | Monetary Gain | Extortionists | Organized Crime |
| Lust | Industrial Espionage | Thrill-Seeking Hackers | Individuals for Thrill | Industrial Espionage |
| Stupidity | Insider Recruitment by Script Kiddies | Script Kiddies | Hacktivist Groups or Script Kiddies | Script Kiddies |
| TTP’s | Data exfiltration, privilege escalation, social engineering, covert communication, evasion of security measures, false flag operations, supply chain compromise | Phishing campaigns, exploit kits, malicious email attachments, lateral movement within networks, encryption of files, ransom demands and payment mechanisms. | Leaking sensitive information, spreading false information through social media, conducting smear campaigns, manipulating online reviews, engaging in cyber-espionage | Exploiting vulnerabilities, phishing attacks, credential stuffing, password cracking, privilege escalation, lateral movement within networks. |