Executive Summary: Threat Model for Metropolis Transit

Overview

As Metropolis Transit integrates and expands its network infrastructure to encompass a range of services and operations, the need for a comprehensive threat model has become paramount. This summary provides an overview of the key security aspects, threats, and vulnerabilities inherent in our current network setup, aiming to inform and guide strategic decisions at the executive level.

Network Infrastructure and Trust Boundaries

Our network architecture, comprising a DMZ, internal subnets (TIS, Enterprise, Garage, Development), and a suite of IoT devices, presents a complex landscape. The DMZ serves as the primary interface with the public internet, hosting externally accessible services. Internal subnets are segmented to isolate and protect various operational functions. Trust boundaries are primarily at the DMZ's edge, within subnet divisions, and around IoT devices, marking transitions in security levels.

Key Adversarial Threats and Motivations

The threat landscape encompasses a variety of potential adversaries, each with distinct motivations:

1. Cybercriminals (Financial Gain, Ego): Targeting financial transactions, data theft.
2. Hacktivists (Ideology): Seeking to disrupt services or deface public-facing assets.
3. Competitors (Economic Advantage): Engaged in corporate espionage.
4. Insiders (Various Motivations): Misusing access for sabotage or data theft.
5. Nation-State Actors (Political, Strategic Goals): Conducting espionage or sophisticated attacks on critical infrastructure.

Vulnerabilities and Risks

Our analysis highlights several key vulnerabilities:

* Legacy Systems (Windows XP, Ubuntu 12.04) in the Garage subnet, posing significant security risks.
* IoT Device Security: Potential for exploitation due to limited direct internet exposure.
* Publicly Accessible Services (HTTP/HTTPS, SMTP, FTP/SFTP) in the DMZ, susceptible to various attack vectors.

Recommended Focus Areas

1. Enhanced Monitoring and Incident Response: Implement advanced monitoring solutions, especially for critical DMZ services and IoT devices.
2. Regular Security Audits and Updates: Prioritize updating and patching legacy systems and regularly review security configurations.
3. Employee Training and Insider Threat Mitigation: Establish comprehensive insider threat programs and regular staff security training.
4. Advanced Threat Protection: Implement layered security measures, including firewalls, intrusion detection/prevention systems, and regular penetration testing.

System Overview

Introduction

Metropolis Transit is a large metropolitan transit corporation formed from the amalgamation of several smaller, local mass transit providers. It aims to unify and modernize its infrastructure for efficient management and operation. As part of this initiative, Metropolis Transit has embarked on developing a comprehensive network infrastructure that supports various functionalities crucial for their operations.

**Network Architecture:**

The network infrastructure of Metropolis Transit is structured into several key components, each serving specific roles:

1. Demilitarized Zone (DMZ) Network:
   * This is a controlled network segment that acts as a buffer zone between the public internet and the internal network of Metropolis Transit. It hosts externally accessible services, ensuring that public traffic does not directly reach the internal network.
   * Key components include routers, DNS servers, web servers, mail servers, FTP and SFTP servers, and a database server.
   * The DMZ network is designed to allow certain services to be accessible from the internet, such as HTTP/HTTPS for web services, SMTP for mail services, and FTP/SFTP for file transfer services, while restricting others.
2. Internet of Things (IoT) Devices:
   * These devices range from point-of-sale systems to ticket readers in buses, integral to passenger management.
   * Although part of the network, these devices are not directly accessible from the internet, enhancing security.
3. Internal Subnets:
   * TIS Subnet: Houses technology information systems essential for corporate operations. Includes servers for Active Directory, security information and event management (SIEM), and data storage.
   * Enterprise Subnet: Primarily consists of workstations used by corporate employees, operating under a dynamic host configuration protocol (DHCP) range.
   * Garage Subnet: Contains older workstations, mainly used for inventory tracking and fleet management. Notable for including legacy systems such as Windows XP and Windows 7.
   * Development Subnet: A flexible environment for developers, hosting systems and code not yet ready for production. Specific details vary based on developmental needs.

**Security Measures:**

The network employs various security measures, such as:

* Firewalls and Routers: To control and monitor traffic entering and exiting the network.
* Segmentation: Subnets are used to segment the network, isolating different types of traffic and reducing the risk of widespread network breaches.
* Restricted Access: Certain services, especially SSH, are restricted to internal IP ranges, limiting remote administrative access.

System decomposition

The system decomposition of Metropolis Transit's network involves analyzing the trust boundaries, entry and exit points, and potential data flows. This analysis is critical for understanding how different components interact and where vulnerabilities might exist.

Trust Boundaries

Trust boundaries are the points in the system where the level of trust or control changes. For Metropolis Transit, these include:

1. DMZ and Internal Network: The DMZ acts as the primary trust boundary between the external internet and the internal network. Systems within the DMZ are exposed to a higher level of risk and are less trusted than those within the internal network.
2. Subnet Divisions: Each subnet (TIS, Enterprise, Garage, Development) represents its own trust boundary within the internal network. The level of trust varies based on the sensitivity and usage of each subnet.
3. IoT Devices: The IoT devices form a unique trust boundary due to their specific functionalities and limited internet exposure.

Entry Points

Entry points are where data or users can enter the system. In Metropolis Transit's network, these include:

1. DMZ Services: Services like HTTP/HTTPS, SMTP, FTP/SFTP, and DNS serve as entry points for external users and data.
2. Remote Access: Remote Desktop Protocol (RDP) and SSH (limited to internal IP ranges) provide controlled entry points for remote administration.
3. Point-of-Sale Systems and Ticket Readers: These IoT devices, though not directly internet-accessible, are entry points for passenger interaction.

Exit Points

Exit points are where data leaves the system. They largely mirror the entry points:

1. Email and Web Services: Data exits through SMTP, HTTP/HTTPS as part of normal operations.
2. File Transfer Services: FTP/SFTP servers facilitate data exit during file transfers.
3. Data Reporting and Exports: From internal subnets, especially in the TIS and Enterprise subnets, data might exit for reporting or external communication purposes.

Data Flows

Understanding the flow of data is essential to identify potential areas of risk:

1. From DMZ to Internal Network: Data flows from the DMZ to internal subnets for processing and storage. This includes web traffic, emails, and file transfers.
2. Within Subnets: Each subnet has its data flow, such as directory services in the TIS subnet and work-related data in the Enterprise subnet.
3. From IoT Devices to Backend Systems: Data collected from IoT devices, like ticketing information, flows into the internal network for processing and analysis.
4. External Data Interactions: Interactions with external entities, such as cloud services or other transit systems, involve data flow across the network boundary.

Adversary Analysis

Introduction

In analyzing potential adversaries for Metropolis Transit's systems, we consider their motivations and the tactics, techniques, and procedures (TTPs) they might employ. We use the MICE (Money, Ideology, Coercion, Ego) and RASCLS (Reconnaissance, Access, Subversion, Command, Lateral movement, Sustainment) frameworks to understand their motivations and methods.

Types of Adversaries and Their Motivations

1. Cybercriminals (Money, Ego)
   * Motivated by financial gain or personal achievement.
   * Likely to target financial transactions, such as point-of-sale systems, or attempt ransomware attacks on critical infrastructure.
2. Hacktivists (Ideology)

* Driven by ideological beliefs, possibly targeting Metropolis Transit due to its public nature or policies.
* May attempt to deface websites or disrupt services to make a statement.

1. Competing Companies (Money, Coercion)

* Motivated by economic competition, could seek to undermine Metropolis Transit's operations or steal sensitive information.
* Industrial espionage, such as stealing strategic plans or financial data, could be a key tactic.

1. Insider Threats (All MICE factors)

* Employees or contractors with access to the system, motivated by various personal reasons, including dissatisfaction, financial gain, or coercion.
* Could misuse their access to leak information, sabotage systems, or facilitate external attacks.

1. Nation-State Actors (Ideology, Coercion)

* Motivated by political or strategic objectives.
* Advanced persistent threats (APTs) targeting critical infrastructure or espionage activities are potential concerns.

Likely TTPs Employed

1. Cybercriminals
   * Reconnaissance: Scanning for vulnerabilities in internet-facing services.
   * Access: Exploiting weak points, phishing attacks.
   * Lateral Movement: Spreading across the network to access financial systems or sensitive data.
   * Sustainment: Installing backdoors for continued access.
2. Hacktivists
   * Reconnaissance: Identifying high-visibility targets.
   * Subversion: Website defacement, DDoS attacks.
   * Command: Leveraging social media for orchestrated attacks.
3. Competing Companies
   * Access: Social engineering, insider threats.
   * Subversion: Installing spyware or keyloggers.
   * Lateral Movement: Moving discreetly to avoid detection.
4. Insider Threats
   * Access: Misusing legitimate credentials.
   * Subversion: Altering or deleting data.
   * Command and Lateral Movement: Utilizing insider knowledge for targeted attacks.
5. Nation-State Actors
   * Reconnaissance: Advanced intelligence gathering.
   * Access and Sustainment: Long-term infiltration strategies.
   * Lateral Movement: Accessing critical systems.
   * Command: Stealth and sophisticated techniques for specific goals.

Threats:

1. DMZ Network:
   * **router1.metropolistransit.net:**

1. Spoofing:

- Threat: Unauthorized access to the router1.metropolistransit.net.

- Attack Graph: Attacker gains access to the LAN by impersonating a legitimate user or device. This could be achieved through password cracking, credential theft, or exploiting vulnerabilities in authentication mechanisms.

2. Tampering:

- Threat: Unauthorized modification of router1.metropolistransit.net configuration.

- Attack Graph: Attacker gains access to the LAN and modifies the router configuration. This could lead to unauthorized access, traffic redirection, or disruption of network services.

3. Repudiation:

- Threat: Denial of responsibility for actions on router1.metropolistransit.net.

- Attack Graph: Attacker gains access to the LAN, performs malicious actions, and attempts to cover their tracks by deleting or altering log files or activity records to avoid detection.

4. Information Disclosure:

- Threat: Unauthorized access to sensitive information on the LAN.

- Attack Graph: Attacker gains access to the LAN and extracts sensitive information from the router or other devices. This could include configuration details, user credentials, or network topology.

5. Denial of Service (DoS):

- Threat: Disruption of HTTP, HTTPS, or SSH services on the LAN.

- Attack Graph: Attacker launches a DoS attack against the LAN, overwhelming the network or services to make them unavailable to legitimate users.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on router1.metropolistransit.net.

- Attack Graph: Attacker gains access to the LAN with lower privileges and exploits vulnerabilities to elevate their privileges, gaining control over the router or other critical network components.

* + **ns1.metropolistransit.net:**

1. Spoofing:

- Threat: Unauthorized access to ns1.metropolistransit.net DNS server.

- Attack Graph: Attacker spoofs their identity to gain unauthorized access to the DNS server. This could involve IP or DNS spoofing, allowing the attacker to impersonate a trusted entity and potentially manipulate DNS records.

2. Tampering:

- Threat: Unauthorized modification of DNS records on ns1.metropolistransit.net.

- Attack Graph: Attacker gains access to the DNS server and modifies DNS records, redirecting traffic to malicious sites or causing communication disruptions within the network.

3. Repudiation:

- Threat: Denial of responsibility for DNS changes on ns1.metropolistransit.net.

- Attack Graph: Attacker gains access to the DNS server, alters records, and attempts to cover their tracks by deleting or modifying logs to avoid detection.

4. Information Disclosure:

- Threat: Unauthorized access to DNS-related information on ns1.metropolistransit.net.

- Attack Graph: Attacker gains access to the DNS server and extracts sensitive information, such as domain configurations, IP addresses, or network topology.

5. Denial of Service (DoS):

- Threat: Disruption of DNS services on ns1.metropolistransit.net.

- Attack Graph: Attacker launches a DoS attack against the DNS server, overwhelming it with requests or exploiting vulnerabilities to make it unavailable, disrupting normal network operations.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on ns1.metropolistransit.net.

- Attack Graph: Attacker gains access to the DNS server with lower privileges and exploits vulnerabilities to elevate their privileges, potentially gaining control over the DNS configuration and records.

* + **ns2.metropolistransit.net:**

1. Spoofing:

- Threat: Unauthorized access to ns2.metropolistransit.net DNS server.

- Attack Graph: Attacker spoofs their identity to gain unauthorized access to the DNS server. This could involve IP or DNS spoofing, allowing the attacker to impersonate a trusted entity and potentially manipulate DNS records.

2. Tampering:

- Threat: Unauthorized modification of DNS records on ns2.metropolistransit.net.

- Attack Graph: Attacker gains access to the DNS server and modifies DNS records, redirecting traffic to malicious sites or causing communication disruptions within the network.

3. Repudiation:

- Threat: Denial of responsibility for DNS changes on ns2.metropolistransit.net.

- Attack Graph: Attacker gains access to the DNS server, alters records, and attempts to cover their tracks by deleting or modifying logs to avoid detection.

4. Information Disclosure:

- Threat: Unauthorized access to DNS-related information on ns2.metropolistransit.net.

- Attack Graph: Attacker gains access to the DNS server and extracts sensitive information, such as domain configurations, IP addresses, or network topology.

5. Denial of Service (DoS):

- Threat: Disruption of DNS services on ns2.metropolistransit.net.

- Attack Graph: Attacker launches a DoS attack against the DNS server, overwhelming it with requests or exploiting vulnerabilities to make it unavailable, disrupting normal network operations.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on ns2.metropolistransit.net.

- Attack Graph: Attacker gains access to the DNS server with lower privileges and exploits vulnerabilities to elevate their privileges, potentially gaining control over the DNS configuration and records.

* + **www.metropolistransit.net:**

1. Spoofing:

- Threat: Impersonation of www.metropolistransit.net.

- Attack Graph: Attacker impersonates the website using DNS spoofing or other means, leading to potential unauthorized access or data interception.

2. Tampering:

- Threat: Unauthorized modification of website content.

- Attack Graph: Attacker gains access and alters the website content, potentially leading to the distribution of malicious content to users.

3. Repudiation:

- Threat: Denial of responsibility for web content changes.

- Attack Graph: Attacker modifies the website and attempts to cover their tracks, making it difficult to trace the changes back to them.

4. Information Disclosure:

- Threat: Exposure of sensitive information through the website.

- Attack Graph: Attacker exploits vulnerabilities to gain access and extract sensitive information hosted on the website.

5. Denial of Service (DoS):

- Threat: Disruption of HTTP, HTTPS services on www.metropolistransit.net.

- Attack Graph: Attacker launches a DoS attack, overwhelming the web server and making it unavailable to legitimate users.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on www.metropolistransit.net.

- Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the web server, potentially compromising the entire system.

* + **mail.metropolistransit.net:**

1. Spoofing:

- Threat: Impersonation of mail.metropolistransit.net.

- Attack Graph: An attacker could attempt DNS spoofing to redirect traffic to a malicious server impersonating mail.metropolistransit.net, leading to unauthorized access or interception of email and other services.

2. Tampering:

- Threat: Unauthorized modification of email content or web traffic.

- Attack Graph: An attacker gains access to the server, altering emails during transit or manipulating web content served by the HTTP or HTTPS services, potentially leading to dissemination of false information or data manipulation.

3. Repudiation:

- Threat: Denial of responsibility for email or web content changes.

- Attack Graph: An attacker modifies emails or web content and attempts to cover their tracks by deleting or altering logs, making it challenging to attribute the changes to a specific user or source.

4. Information Disclosure:

- Threat: Exposure of sensitive information through email or web services.

- Attack Graph: An attacker exploits vulnerabilities to gain access to email communications, extract sensitive information, or intercept data transmitted via HTTP or HTTPS.

5. Denial of Service (DoS):

- Threat: Disruption of SMTP, IMAP, POP3, HTTP, or HTTPS services.

- Attack Graph: An attacker launches a DoS attack against the server, overwhelming it with traffic, making it temporarily or permanently unavailable for legitimate users.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on the mail server.

- Attack Graph: An attacker exploits vulnerabilities in the Ubuntu 16.04 operating system or associated services, gaining elevated access on the server and potentially compromising the entire system.

* + **ftp.metropolistransit.net:**

1. Spoofing:

- Threat: Impersonation of ftp.metropolistransit.net.

- Attack Graph: Attacker impersonates the FTP server, leading to potential unauthorized access or interception of data during file transfers.

2. Tampering:

- Threat: Unauthorized modification of files during FTP transfers.

- Attack Graph: Attacker gains access and alters files during FTP transfers, potentially leading to data manipulation or dissemination of malicious content.

3. Repudiation:

- Threat: Denial of responsibility for FTP file changes.

- Attack Graph: Attacker modifies files during FTP transfers and attempts to cover their tracks, making it difficult to trace the changes back to them.

4. Information Disclosure:

- Threat: Exposure of sensitive information through FTP transfers.

- Attack Graph: Attacker exploits vulnerabilities to gain access and extract sensitive information from FTP transfers.

5. Denial of Service (DoS):

- Threat: Disruption of FTP services on ftp.metropolistransit.net.

- Attack Graph: Attacker launches a DoS attack, overwhelming the FTP server and making it unavailable to legitimate users.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on ftp.metropolistransit.net.

- Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the FTP server, potentially compromising the entire system.

* + **www2.metropolistransit.net:**

1. Spoofing:

- Threat: Impersonation of www2.metropolistransit.net.

- Attack Graph: Attacker impersonates the website using DNS spoofing or other means, leading to potential unauthorized access or data interception.

2. Tampering:

- Threat: Unauthorized modification of website content.

- Attack Graph: Attacker gains access and alters the website content, potentially leading to the distribution of malicious content to users.

3. Repudiation:

- Threat: Denial of responsibility for web content changes.

- Attack Graph: Attacker modifies the website and attempts to cover their tracks, making it difficult to trace the changes back to them.

4. Information Disclosure:

- Threat: Exposure of sensitive information through the website.

- Attack Graph: Attacker exploits vulnerabilities to gain access and extract sensitive information hosted on the website.

5. Denial of Service (DoS):

- Threat: Disruption of HTTP, HTTPS services on www2.metropolistransit.net.

- Attack Graph: Attacker launches a DoS attack, overwhelming the web server and making it unavailable to legitimate users.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on www2.metropolistransit.net.

- Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the web server, potentially compromising the entire system.

* + **api.metropolistransit.net:**

1. Spoofing:

- Threat: Impersonation of api.metropolistransit.net.

- Attack Graph: Attacker impersonates the API server, leading to potential unauthorized access or interception of data during API communications.

2. Tampering:

- Threat: Unauthorized modification of data through API calls.

- Attack Graph: Attacker gains access and alters data during API calls, potentially leading to data manipulation or dissemination of malicious content.

3. Repudiation:

- Threat: Denial of responsibility for API data changes.

- Attack Graph: Attacker modifies data through API calls and attempts to cover their tracks, making it difficult to trace the changes back to them.

4. Information Disclosure:

- Threat: Exposure of sensitive information through API communications.

- Attack Graph: Attacker exploits vulnerabilities to gain access and extract sensitive information from API communications.

5. Denial of Service (DoS):

- Threat: Disruption of API services on api.metropolistransit.net.

- Attack Graph: Attacker launches

a DoS attack, overwhelming the API server and making it unavailable to legitimate users.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on api.metropolistransit.net.

- Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the API server, potentially compromising the entire system.

* + **sftp.metropolistransit.net:**

1. Spoofing:

- Threat: Impersonation of sftp.metropolistransit.net.

- Attack Graph: Attacker impersonates the SFTP server, leading to potential unauthorized access or interception of data during secure file transfers.

2. Tampering:

- Threat: Unauthorized modification of files during SFTP transfers.

- Attack Graph: Attacker gains access and alters files during SFTP transfers, potentially leading to data manipulation or dissemination of malicious content.

3. Repudiation:

- Threat: Denial of responsibility for SFTP file changes.

- Attack Graph: Attacker modifies files during SFTP transfers and attempts to cover their tracks, making it difficult to trace the changes back to them.

4. Information Disclosure:

- Threat: Exposure of sensitive information through SFTP transfers.

- Attack Graph: Attacker exploits vulnerabilities to gain access and extract sensitive information from SFTP transfers.

5. Denial of Service (DoS):

- Threat: Disruption of SFTP services on sftp.metropolistransit.net.

- Attack Graph: Attacker launches a DoS attack, overwhelming the SFTP server and making it unavailable to legitimate users.

6. Elevation of Privilege:

- Threat: Unauthorized escalation of privileges on sftp.metropolistransit.net.

- Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the SFTP server, potentially compromising the entire system.

**Router 2 (10.1.255.1):**

1. Spoofing:

Threat: Unauthorized access to Router2 by spoofing IP addresses.

Attack Graph: Attacker impersonates a legitimate device, gaining unauthorized access to Router2 (10.1.255.1).

2. Tampering:

Threat: Unauthorized modification of Router2 configuration.

Attack Graph: Attacker gains access to Router2 and alters its configuration, potentially leading to unauthorized access or network disruption.

3. Repudiation:

Threat: Denial of responsibility for actions on Router2.

Attack Graph: Attacker gains access, performs malicious actions, and covers tracks by deleting or altering logs on Router2.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on Router2.

Attack Graph: Attacker gains access to Router2 and extracts sensitive information, compromising confidentiality.

5. Denial of Service (DoS):

Threat: Disruption of SSH, HTTP, HTTPS, or DNS services on Router2.

Attack Graph: Attacker launches a DoS attack, overwhelming Router2 services to make them unavailable.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on Router2.

Attack Graph: Attacker gains access with lower privileges, exploits vulnerabilities to gain control over Router2.

**CEO's Windows 10 Machine (ceo.metropolistransit.net, 192.168.207.10):**

1. Spoofing:

Threat: Unauthorized access to the CEO's Windows 10 machine.

Attack Graph: Attacker impersonates a legitimate user, gaining unauthorized access to the CEO's Windows 10 machine.

2. Tampering:

Threat: Unauthorized modification of the CEO's Windows 10 machine.

Attack Graph: Attacker gains access and alters configurations or data on the CEO's Windows 10 machine.

3. Repudiation:

Threat: Denial of responsibility for actions on the CEO's Windows 10 machine.

Attack Graph: Attacker gains access, performs actions, and attempts to cover tracks by deleting or altering logs.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on the CEO's Windows 10 machine.

Attack Graph: Attacker gains access and extracts sensitive information, compromising confidentiality.

5. Denial of Service (DoS):

Threat: Disruption of RDP services on the CEO's Windows 10 machine.

Attack Graph: Attacker launches a DoS attack, making RDP services temporarily or permanently unavailable.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on the CEO's Windows 10 machine.

Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the CEO's Windows 10 machine.

**Ubuntu 14.04 IoT Devices (10.1.10.1-200):**

1. Spoofing:

Threat: Unauthorized access to Ubuntu 14.04 IoT devices (e.g., 10.1.10.1).

Attack Graph: Attacker impersonates a legitimate device, gaining unauthorized access to the IoT devices.

2. Tampering:

Threat: Unauthorized modification of data on Ubuntu 14.04 IoT devices (e.g., 10.1.10.1).

Attack Graph: Attacker gains access and alters data on the IoT device, potentially causing data manipulation.

3. Repudiation:

Threat: Denial of responsibility for actions on Ubuntu 14.04 IoT devices (e.g., 10.1.10.1).

Attack Graph: Attacker gains access, performs actions, and attempts to cover tracks to avoid detection.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on Ubuntu 14.04 IoT devices (e.g., 10.1.10.1).

Attack Graph: Attacker gains access and extracts sensitive information from the IoT devices.

5. Denial of Service (DoS):

Threat: Disruption of SSH services on Ubuntu 14.04 IoT devices (e.g., 10.1.10.1).

Attack Graph: Attacker launches a DoS attack, overwhelming SSH services on the IoT devices.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on Ubuntu 14.04 IoT devices (e.g., 10.1.10.1).

Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the IoT device.

TIS Subnet:

**Router 2 (TIS Subnet) (192.168.0.1):**

1. Spoofing:

Threat: Unauthorized access to Router 2 (192.168.0.1) in the TIS Subnet.

Attack Graph: Attacker spoofs their identity to gain unauthorized access to Router 2 in the TIS Subnet, potentially using IP or MAC address spoofing.

2. Tampering:

Threat: Unauthorized modification of Router 2 (192.168.0.1) configuration.

Attack Graph: Attacker gains access to Router 2 and modifies its configuration, leading to unauthorized access, traffic redirection, or disruption of network services within the TIS Subnet.

3. Repudiation:

Threat: Denial of responsibility for actions on Router 2 (192.168.0.1) in the TIS Subnet.

Attack Graph: Attacker gains access to Router 2, performs malicious actions, and attempts to cover their tracks by deleting or altering log files to avoid detection within the TIS Subnet.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on Router 2 (192.168.0.1) in the TIS Subnet.

Attack Graph: Attacker gains access to Router 2 and extracts sensitive information, such as configuration details or network topology, compromising the confidentiality of the TIS Subnet.

5. Denial of Service (DoS):

Threat: Disruption of SSH, HTTP, HTTPS, or DNS services on Router 2 (192.168.0.1) in the TIS Subnet.

Attack Graph: Attacker launches a DoS attack against Router 2 services, overwhelming the network or services to make them unavailable within the TIS Subnet.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on Router 2 (192.168.0.1) in the TIS Subnet.

Attack Graph: Attacker gains access to Router 2 with lower privileges and exploits vulnerabilities to elevate their privileges, potentially gaining control over the router or other critical network components within the TIS Subnet.

**SIEM Server (siem.metropolistransit.net) (192.168.0.3):**

1. Spoofing:

Threat: Unauthorized access to the SIEM server (192.168.0.3) in the TIS Subnet.

Attack Graph: Attacker spoofs their identity to gain unauthorized access to the SIEM server, potentially using IP or MAC address spoofing.

2. Tampering:

Threat: Unauthorized modification of SIEM server (192.168.0.3) configurations.

Attack Graph: Attacker gains access to the SIEM server and modifies configurations, leading to unauthorized changes or disruptions in the TIS Subnet.

3. Repudiation:

Threat: Denial of responsibility for actions on the SIEM server (192.168.0.3) in the TIS Subnet.

Attack Graph: Attacker gains access, performs actions, and attempts to cover tracks by deleting or altering logs, making it challenging to attribute changes within the TIS Subnet.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on the SIEM server (192.168.0.3) in the TIS Subnet.

Attack Graph: Attacker gains access to the SIEM server and extracts sensitive information, such as logs or network events, compromising the confidentiality of the TIS Subnet.

5. Denial of Service (DoS):

Threat: Disruption of OSSIM services on the SIEM server (192.168.0.3) in the TIS Subnet.

Attack Graph: Attacker launches a DoS attack, overwhelming the SIEM server with requests, making it temporarily or permanently unavailable within the TIS Subnet.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on the SIEM server (192.168.0.3) in the TIS Subnet.

Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the SIEM server, potentially compromising the entire TIS Subnet.

**Warehouse Server (warehouse.metropolistransit.net) (192.168.0.4):**

1. Spoofing:

Threat: Unauthorized access to the Warehouse Server (192.168.0.4) in the TIS Subnet.

Attack Graph: Attacker spoofs their identity to gain unauthorized access to the Warehouse Server, potentially using IP or MAC address spoofing.

2. Tampering:

Threat: Unauthorized modification of Warehouse Server (192.168.0.4) configurations.

Attack Graph: Attacker gains access to the Warehouse Server and modifies configurations, leading to unauthorized changes or disruptions in the TIS Subnet.

3. Repudiation:

Threat: Denial of responsibility for actions on the Warehouse Server (192.168.0.4) in the TIS Subnet.

Attack Graph: Attacker gains access, performs actions, and attempts to cover tracks by deleting or altering logs, making it challenging to attribute changes within the TIS Subnet.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on the Warehouse Server (192.168.0.4) in the TIS Subnet.

Attack Graph: Attacker gains access to the Warehouse Server and extracts sensitive information, such as inventory data or MySQL databases, compromising the confidentiality of the TIS Subnet.

5. Denial of Service (DoS):

Threat: Disruption of SSH, MySQL services on the Warehouse Server (192.168.0.4) in the TIS Subnet.

Attack Graph: Attacker launches a DoS attack, overwhelming the Warehouse Server with requests, making it temporarily or permanently unavailable within the TIS Subnet.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on the Warehouse Server (192.168.0.4) in the TIS Subnet.

Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the Warehouse Server, potentially compromising the entire TIS Subnet.

Enterprise Subnet:

**Router 2 (Enterprise Subnet) (192.168.1.1):**

1. Spoofing:

Threat: Unauthorized access to Router 2 (192.168.1.1) in the Enterprise Subnet.

Attack Graph: Attacker spoofs their identity to gain unauthorized access to Router 2 in the Enterprise Subnet, potentially using IP or MAC address spoofing.

2. Tampering:

Threat: Unauthorized modification of Router 2 (192.168.1.1) configuration.

Attack Graph: Attacker gains access to Router 2 and modifies its configuration, leading to unauthorized access, traffic redirection, or disruption of network services within the Enterprise Subnet.

3. Repudiation:

Threat: Denial of responsibility for actions on Router 2 (192.168.1.1) in the Enterprise Subnet.

Attack Graph: Attacker gains access to Router 2, performs malicious actions, and attempts to cover their tracks by deleting or altering log files to avoid detection within the Enterprise Subnet.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on Router 2 (192.168.1.1) in the Enterprise Subnet.

Attack Graph: Attacker gains access to Router 2 and extracts sensitive information, such as configuration details or network topology, compromising the confidentiality of the Enterprise Subnet.

5. Denial of Service (DoS):

Threat: Disruption of SSH, HTTP, HTTPS, or DNS services on Router 2 (192.168.1.1) in the Enterprise Subnet.

Attack Graph: Attacker launches a DoS attack against Router 2 services, overwhelming the network or services to make them unavailable within the Enterprise Subnet.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on Router 2 (192.168.1.1) in the Enterprise Subnet.

Attack Graph: Attacker gains access to Router 2 with lower privileges and exploits vulnerabilities to elevate their privileges, potentially gaining control over the router or other critical network components within the Enterprise Subnet.

**DHCP Server (Enterprise Subnet) (192.168.1.10-255):**

1. Spoofing:

Threat: Unauthorized access to the DHCP Server (192.168.1.10-255) in the Enterprise Subnet.

Attack Graph: Attacker spoofs their identity to gain unauthorized access to the DHCP Server, potentially using IP or MAC address spoofing.

2. Tampering:

Threat: Unauthorized modification of DHCP Server configurations.

Attack Graph: Attacker gains access to the DHCP Server and modifies configurations, leading to unauthorized changes or disruptions in the assignment of IP addresses within the Enterprise Subnet.

3. Repudiation:

Threat: Denial of responsibility for actions on the DHCP Server in the Enterprise Subnet.

Attack Graph: Attacker gains access, performs malicious actions, and attempts to cover tracks by deleting or altering logs, making it challenging to attribute changes within the Enterprise Subnet.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on the DHCP Server in the Enterprise Subnet.

Attack Graph: Attacker gains access to the DHCP Server and extracts sensitive information, such as assigned IP addresses or lease information, compromising the confidentiality of the Enterprise Subnet.

5. Denial of Service (DoS):

Threat: Disruption of DHCP services in the Enterprise Subnet.

Attack Graph: Attacker launches a DoS attack against the DHCP Server, overwhelming it with requests or exploiting vulnerabilities to make it unavailable, disrupting normal network operations within the Enterprise Subnet.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on the DHCP Server in the Enterprise Subnet.

Attack Graph: Attacker exploits vulnerabilities to gain elevated access on the DHCP Server, potentially compromising the entire Enterprise Subnet.

Garage Subnet:

**Router 2 (Garage Subnet) (192.168.2.1):**

1. Spoofing:

Threat: Unauthorized access to Router 2 (192.168.2.1) in the Garage Subnet.

Attack Graph: Attacker spoofs their identity to gain unauthorized access to Router 2 in the Garage Subnet, potentially using IP or MAC address spoofing.

2. Tampering:

Threat: Unauthorized modification of Router 2 (192.168.2.1) configuration.

Attack Graph: Attacker gains access to Router 2 and modifies its configuration, leading to unauthorized access, traffic redirection, or disruption of network services within the Garage Subnet.

3. Repudiation:

Threat: Denial of responsibility for actions on Router 2 (192.168.2.1) in the Garage Subnet.

Attack Graph: Attacker gains access to Router 2, performs malicious actions, and attempts to cover their tracks by deleting or altering log files to avoid detection within the Garage Subnet.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on Router 2 (192.168.2.1) in the Garage Subnet.

Attack Graph: Attacker gains access to Router 2 and extracts sensitive information, such as configuration details or network topology, compromising the confidentiality of the Garage Subnet.

5. Denial of Service (DoS):

Threat: Disruption of SSH, HTTP, HTTPS, or DNS services on Router 2 (192.168.2.1) in the Garage Subnet.

Attack Graph: Attacker launches a DoS attack against Router 2 services, overwhelming the network or services to make them unavailable within the Garage Subnet.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on Router 2 (192.168.2.1) in the Garage Subnet.

**DHCP Server (Garage Subnet) (192.168.2.10-255):**

1. Spoofing:

Threat: Unauthorized access to the DHCP Server (192.168.2.10-255) in the Garage Subnet.

Attack Graph: Attacker spoofs their identity to gain unauthorized access to the DHCP Server, potentially using IP or MAC address spoofing.

2. Tampering:

Threat: Unauthorized modification of DHCP Server configurations.

Attack Graph: Attacker gains access to the DHCP Server and modifies configurations, leading to unauthorized changes or disruptions in the assignment of IP addresses within the Garage Subnet.

3. Repudiation:

Threat: Denial of responsibility for actions on the DHCP Server in the Garage Subnet.

Attack Graph: Attacker gains access, performs malicious actions, and attempts to cover tracks by deleting or altering logs, making it challenging to attribute changes within the Garage Subnet.

4. Information Disclosure:

Threat: Unauthorized access to sensitive information on the DHCP Server in the Garage Subnet.

Attack Graph: Attacker gains access to the DHCP Server and extracts sensitive information, such as assigned IP addresses or lease information, compromising the confidentiality of the Garage Subnet.

5. Denial of Service (DoS):

Threat: Disruption of DHCP services in the Garage Subnet.

Attack Graph: Attacker launches a DoS attack against the DHCP Server, overwhelming it with requests or exploiting vulnerabilities to make it unavailable, disrupting normal network operations within the Garage Subnet.

6. Elevation of Privilege:

Threat: Unauthorized escalation of privileges on the DHCP Server in the Garage Subnet.

Vulnerabilities:

Here's a summary of potential vulnerabilities in the environment based on the described systems:

1. Weak Authentication:

- Systems Impacted: All systems

- Impact: Unauthorized access to the systems could lead to data breaches, service disruptions, or unauthorized modifications.

2. Unpatched Software:

- Systems Impacted: All systems

- Impact: Vulnerabilities in software could be exploited by attackers to gain unauthorized access, tamper with data, or launch denial of service attacks.

3. DNS Spoofing:

- Systems Impacted: All systems

- Impact: Impersonation of these services could lead to unauthorized access or manipulation of data.

4. Unauthorized DNS Changes:

- Systems Impacted: All systems

- Impact: Tampering with DNS records could redirect traffic, leading to potential data interception or service disruption.

5. Information Disclosure:

- Systems Impacted: All systems

- Impact: Unauthorized access to sensitive information on these systems could lead to data breaches and privacy violations.

6. Denial of Service (DoS) Threats:

- Systems Impacted: All systems

- Impact: Disruption of services, leading to potential downtime and loss of availability.

7. Elevation of Privilege:

- Systems Impacted: All systems

- Impact: Unauthorized escalation of privileges could lead to full control over the compromised systems.

8. Firewall Configuration Issues:

- Systems Impacted: All systems

- Impact: Misconfigurations in the firewall rules may inadvertently allow unauthorized access or disrupt legitimate services.

9. Insufficient Monitoring:

- Systems Impacted: All systems

- Impact: Lack of proper monitoring may delay the detection of security incidents, allowing attackers to persist undetected.

10. Overlooking Physical Security:

- Systems Impacted: All systems

- Impact: Inadequate physical security measures could lead to unauthorized access to servers, potentially compromising the entire environment.

Mitigation Strategies:

- Implement strong authentication mechanisms.

- Regularly update and patch software.

- Monitor DNS for any unauthorized changes.

- Encrypt sensitive information to prevent unauthorized disclosure.

- Implement proper firewall configurations and access controls.

- Conduct regular security assessments and audits.

- Educate users on secure practices.

- Establish and enforce physical security measures for server locations.

Addressing these vulnerabilities will require a holistic approach, combining technical measures, user education, and ongoing monitoring to ensure a robust and secure environment.