**Implementing Cybersecurity Tools, Techniques, and Procedures in Mumbai's Local Transport System**

# Introduction

Mumbai, the financial capital of India, is a densely populated city, and its local transport system plays a crucial role in the daily lives of its residents. With more than 20 million people relying on various modes of public transportation, including trains, buses, and taxis, the city's transport network is often referred to as the "lifeline of Mumbai”. The local trains alone carry over 6 million passengers daily with pre-pandemic numbers being as high as 8 million passengers (The Indian Express, 2022), highlighting the importance of an efficient and secure public transportation system.

In today's interconnected world, public transportation systems are increasingly reliant on digital technologies and information systems for their operations, including ticketing, passenger information, and traffic management. As a result, these systems have become more susceptible to cyberattacks, which pose significant risks to the safety, privacy, and operational efficiency of public transport services. Therefore, it is crucial to implement robust cybersecurity tools, techniques, and procedures to safeguard Mumbai's local transport system from potential threats.

This literature study seeks to investigate the use of cybersecurity technologies, tactics, and processes to improve the security and resilience of the transportation system. Given the limit and the depth we seek for this review, we will only be covering the following topics as key focus areas: [A full list of actionable areas are listed in **Annex I** at the end of this paper]

|  |  |
| --- | --- |
| **Focus Areas** | |
| * Vulnerability Management * Penetration Testing | * Security Audits * Password Management |

# Vulnerability Management

Rapid7, a pioneer in the cybersecurity industry, defines Vulnerability management as: “Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their “attack surface.”” (Rapid7, 2020)

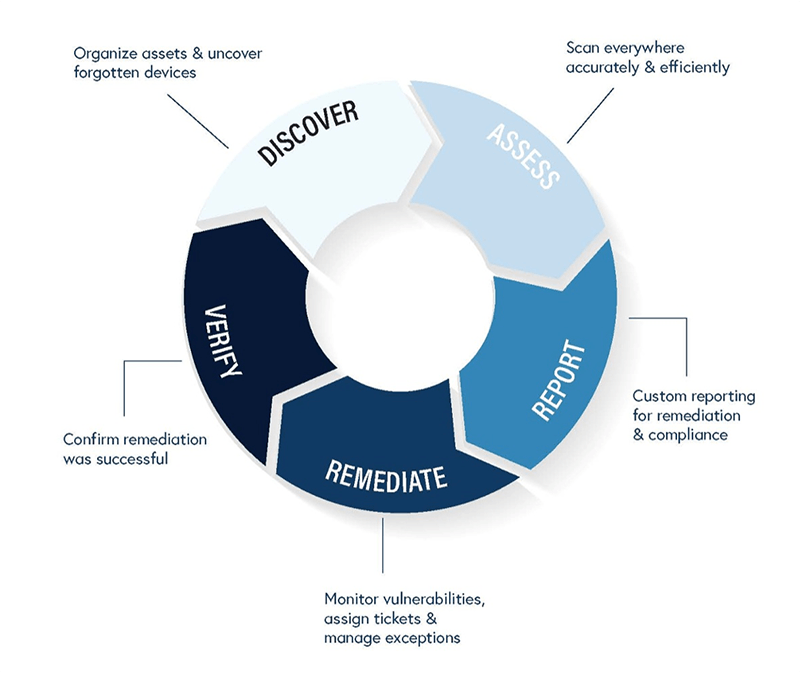


Figure : Key Stages of a Vulnerability Management Process (TeamAscend, n.d.)

This breaks down the process into 5 key steps:

1. **Discover:** Vulnerability scanners are capable of identifying desktops, laptops, virtualized and physical servers, databases, firewalls as well as switches, printers, and more. Operating system, ports, software, user accounts, file system structure, system settings, and more are examined on identified systems. This information links known vulnerabilities to scanned systems. Vulnerability scanners employ a vulnerability and exploitation database to associate publicly known vulnerabilities.
2. **Assess:** An organization's vulnerability management plan must assess vulnerabilities to mitigate risks. Vulnerability management systems calculate risk and CVSS ratings. These rankings help organizations target vulnerabilities, and other elements to determine risk.
3. **Report:** Once a vulnerability has been validated and deemed a risk, the next step is prioritizing how to treat that vulnerability with original stakeholders to the business or network.
4. **Remediate:** **Treating vulnerabilities includes:**
   1. Remediation: Fully addressing or patching a vulnerability to prevent exploitation.
   2. Mitigation: Reducing vulnerability exploitability, when a vulnerability has no patch available.
   3. Acceptance: Not fixing or mitigating a vulnerability. When a vulnerability has low risk and correcting it costs more than exploiting it, this is justifiable.
5. **Verify:** Regular vulnerability assessments help organisations track the pace and efficiency of their vulnerability management programme. Vulnerability management systems provide customisable reports and dashboards for exporting and visualising vulnerability scan results. This helps IT teams easily understand which remediation techniques will help them fix the most vulnerabilities with the least effort.

From personal experiences, I advocate a rigorous vulnerability management methodology for Mumbai’s public transport infrastructure due to its presumed complexity and magnitude. Consider these steps.

* **Having multiple scanners in a variety of network segregations:** Given the widespread nature of public transport systems, the number of operational servers, networks and other infrastructure devices would also be widespread. A single scanner would prove to be a time-consuming task, thus, employing multiple scanners to cover a segment of network would reduce the time and effort to cover the infrastructure end to end.
* **Weekly internal reviews:** Reviewing upon plans is always a good step, it allows to check for how fast you need to go or maintain pace. Covering such a huge infrastructure is a time-consuming task and is not recommended. Periodically scanning the networks by dividing it into zones will allow for timely coverage of the entire infrastructure.
* **Simple remediation timelines:** Most organizations end up complicating the remediation cycle and usually only get into it during their patch cycles. It is recommended that critical and high-risk vulnerabilities be actioned upon immediately leaving low level risks for periodic remediation.

# Penetration Testing

National Cyber Security Centre, defines penetration testing as, “A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.” (National Cyber Security Centre, 2017)

Penetration testing should not be seen as a primary method for identifying vulnerabilities, but rather as a method for obtaining confidence in your organization's vulnerability assessment and management processes.

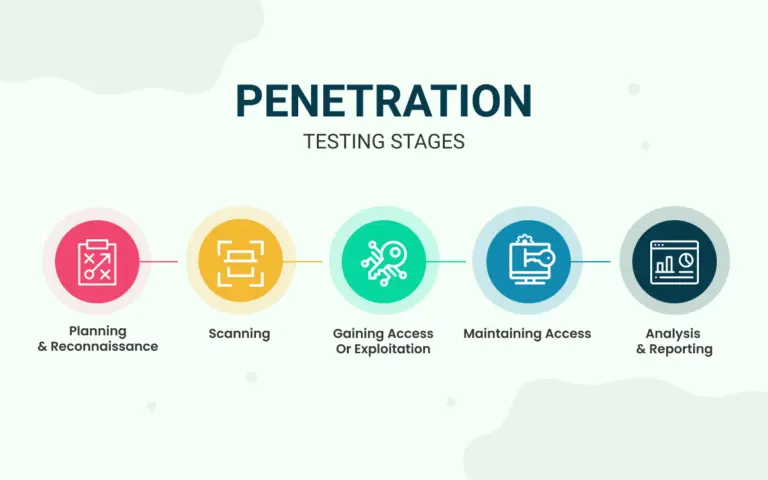


Figure : The 5 Stages of Penetration Testing (Secure Triad, 2021)

The following are the key stages in a penetration test:

1. **Planning and Reconnaissance:** This stage defines scope, priority, and objectives. It also lists the most essential systems and test kinds. To understand how a target functions and its possible entry points, the reconnaissance stage gathers passive and active intelligence on network and domain names, mail servers, etc.
2. **Scanning:** This stage involves understanding how the target system reacts to automated intrusion attempts and techniques in this step.
   1. **Static Analysis (SAST):** Compares application source code against coding guidelines before running a programme to troubleshoot it.
   2. **Dynamic Analysis (DAST):** Real-time data execution tests and evaluates the security system. Automated security scanning technologies are used to discover faults and vulnerabilities in real-time.

Manually verifying vulnerabilities or flaws after static or dynamic analysis eliminates false positives.

1. **Gaining Access or Exploitation:** This step exploits weaknesses to get system or data access. Escalating privileges, stealing data, intercepting communications, and introducing malicious code may be used to assess damage.
2. **Maintaining Access:** This step tests persistence access following application or system access. The attacker acquires greater system access as time goes on. The idea is to mimic and identify sophisticated persistent attacks that frequently go undetected.
3. **Analysis and Reporting:** The test findings are reported in full. The report covers vulnerabilities exploited, sensitive data hacked and accessed, and the security tester's time in the system before detection.

From personal experiences, I advocate a rigorous penetration testing vendor for Mumbai’s public transport infrastructure due to its presumed complexity and magnitude, it may not be possible or necessary to “pentest” everything, however, it is recommended that these testing areas are considered.

* **Web & Mobile Applications:** Applications like the IRCTC Next Generation eTicketing System for interstate travel as well as UTS for local travels are critical infrastructure for the system which allow online and on the go ticket booking. Compromise of such applications can cause both chaos and unprecedented fiscal impact on a national level.
* **IoT Devices:** A lot of these systems are interconnected and are using some form of industrial programmable logical controllers (PLC). Insecurities in these systems and exploitations in such systems could lead to the collapse of the entire system.
* **Cloud Infrastructure:** It is almost impossible to run such a huge network of data operations and infrastructure without the help of assisted computing a.k.a cloud infrastructure, where a lot of the handling and responsibility is passed on to the service provider. Pentesting this will allow for revealing of any exposed secret keys, public buckets like S3 and blob, etc. which must be safeguarded to increase overall resilience of the interconnected systems.

# Security Audits

A security audit is a detailed assessment of the organization’s information system and controls; typically, this assessment examines information system’s security against an audit checklist of industry best practices, externally established standards, or federal regulations. A comprehensive security audit will assess an organization’s security controls relating to the following:

1. Physical infrastructure of the system and the environment in which the system is housed.
2. Applications and software, including but not limited to security patches of systems and their statuses.
3. Network & data, including evaluations of information and how it travels between different points within, and external of, the organization’s network and stored at rest.
4. The human dimension, including how employees collect, share, and store highly sensitive information.

A security audit will map the organization's primary information security flaws and show where it meets and doesn't match its standards. Organisations that handle private data need security audits to evaluate risk and mitigate it.

Given the huge employment provide by Mumbai’s public transport system, and the size of operations, a robust security audit in this case must include:

1. **The right regulatory framework:** External standards include federal guidelines such as the Sarbanes-Oxley Act (SOX), as well as standards established by the International Organisation for Standardisation (ISO) and the National Institute of Standards and Technology (NIST). An audit of security compares the organization's actual IT implmentations adheres to the entity-specific standards and identifies areas for improvement and expansion.
2. **Review network and data access log:** Observe network activity and records of events. Keeping a close eye on records will help ensure that only employees with the appropriate permissions are accessing restricted data, and that those employees are taking the necessary security precautions.
3. **Verification of access:** The larger the number of individuals with access to highly confidential information, the greater the likelihood of human error. Ensure there is a record of how many staff members have undergone training, trained in safeguarding risks or compliance practises and who has access to sensitive information. Prepare for training those who remain untrained.
4. **Applications and software verification:** A security audit should reveal some of your most prominent vulnerabilities, such as if a security patch is out of date or if an application framework version update was never performed, etc. Regular security audits improve the efficiency and effectiveness of penetration tests and vulnerability assessments.
5. **Frequent audit:** The frequency of audit is usually determined by the size and scope of the organization, though doing it frequently has its benefits, it may not be realistically possible for Mumbai’s public transportation system. Realistically a bi-annual approach would work out in such cases.

# Password Management

Zoho, a popular customer relationship management (CRM) software and defines password management as “password management is a set of principles and best practices to be followed by users while storing and managing passwords in an efficient manner to secure passwords as much as they can to prevent unauthorized access.” (Zoho, 2019)

The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication:

* Something you know, usually a password.
* Something you have, a physical device like cryptographic key token (RSA) for instance.
* Something you are, taking authentication to the human by verifying biometric data like a fingerprint or retina scanners.

For Mumbai’s public transport system, it will be a huge task to manage identities, authentication and authorization for their users. However, given that they handle a magnitude of sensitive information of the public, mission critical systems, operations and processes, credentials must be sufficiently protected. Some possible clean password management directives state:

1. Advanced malicious actors have programmes that scan through millions of dictionary words in multiple languages. steer clear of dictionary words to prevent the business from becoming the target of a dictionary attack campaign.
2. Credentials for privileged users require additional safety measures, such as software for privileged access management. In contrast to personal passwords, privileged credentials must be changed frequently, even after each use for exceptionally valuable credentials. For additional security, these credentials should be supplied and never made visible or readily available to the end user.
3. It is not uncommon for disgruntled former employees to become the organization's worst antagonist. Make it standard procedure to update employee credentials when they depart, so that former employees cannot break the system, or worse, sell their still active credentials to notorious adversaries.
4. Apply non-password-based, advanced methods, such as biometric authentication, to mission-critical systems in addition to privileged identity management.

# Conclusion

Implementing cybersecurity measures not only safeguards Mumbai’s local transport system against existing threats but also enhances its overall resilience to emerging cyber threats. A resilient transport system is better equipped to withstand, respond to, and recover from cyber incidents, ensuring the continuity of services and minimizing disruptions for millions of daily passengers.

Thus, it is crucial for Mumbai's local transport system to continuously assess and improve its cybersecurity posture by proactively addressing potential vulnerabilities, ensuring high standards of security best practices, and sophisticated password management systems can minimize the risk of cyberattacks and maintain the safety, privacy, and operational efficiency of its services.

# References

* Chatterjee, P. and Nath, A. (2014). Information Technology in Public Transports of India – A Ubiquitous Approach. 2(10). Available from: https://www.researchgate.net/publication/268153720\_Information\_Technology\_in\_Public\_Transports\_of\_India\_-\_A\_Ubiquitous\_Approach [Accessed 13 Apr. 2023].
* The Indian Express. (2022). Mumbai local trains see highest ridership since pandemic onset. Available from: https://indianexpress.com/article/cities/mumbai/mumbai-local-trains-see-highest-ridership-since-pandemic-onset-7826370/ [Accessed 13 Apr. 2023].
* Team Ascend (n.d.). Vulnerability Management. teamascend.com. Available from: https://blog.teamascend.com/hs-fs/hubfs/Graphic\_Vulnerability-Management.png?width=800&name=Graphic\_Vulnerability-Management.png [Accessed 14 Apr. 2023].
* Rapid7 (2020). What is Vulnerability Management and Vulnerability Scanning. Rapid7. Available from: https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/ [Accessed 14 Apr. 2023].
* National Cyber Security Centre (2017). Penetration Testing. Ncsc.gov.uk. Available from: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed 16 Apr. 2023].
* Secure Triad (2021). Penetration Testing Stages. securetriad.io. Available from: https://securetriad.io/wp-content/uploads/2021/06/penetration-testing-stags-768x480.png [Accessed 16 Apr. 2023].
* auditboard (2021). What Is a Security Audit? The Basics You Need to Get Started. AuditBoard. Available from: https://www.auditboard.com/blog/what-is-security-audit/ [Accessed 17 Apr. 2023].
* Zoho (2019). What is password management? Zoho. Available from: https://www.zoho.com/vault/educational-content/what-is-password-management.html [Accessed 19 Apr. 2023].
* NIST (2019). NIST Special Publication 800-63-3. Nist.gov. Available from: https://pages.nist.gov/800-63-3/sp800-63-3.html [Accessed 19 Apr. 2023].
* Smith, D. (2022). Top 15 Password Management Best Practices | BeyondTrust. www.beyondtrust.com. Available from: https://www.beyondtrust.com/blog/entry/top-15-password-management-best-practices [Accessed 19 Apr. 2023].

# Annex I

|  |
| --- |
| **Actionable Areas for Mumbai’s Local Transport System** |
| 1. Network Security    1. Firewalls    2. Intrusion Detection Systems (IDS)    3. Intrusion Prevention Systems (IPS) 2. Encryption    1. Data encryption at rest and in transit       1. Advanced Encryption Standard       2. Transport Layer Security    2. Secure communication channels       1. Virtual Private Networks       2. Secure messaging protocols 3. Endpoint Security    1. Antivirus and antimalware software    2. Patch management    3. Device management and access control 4. Security Information and Event Management (SIEM)    1. Real-time monitoring and analysis    2. Incident response and management 5. Employee training and awareness programs    1. Security best practices    2. Social engineering and phishing    3. Physical security awareness    4. Regular training and updates on new threats 6. Incident response plan    1. Roles and responsibilities    2. Incident detection and analysis    3. Incident containment, eradication, and recovery 7. Disaster recovery plan    1. Business continuity planning    2. Backup and redundancy strategies    3. Testing and updating the plan |