Vulnerability Analysis to MSLA ID Technology Infrastructure
Final Report Summary

December 2024

NEXUDATA
Opening new grounds

Table of Content

1. FINAL REPORT SUMMARY

1.1 Objectives of the project

- Identify security weaknesses in the technology infrastructure by running penetration tests and reviewing security configurations.

- Classify the impact and document the vulnerabilities identified in order to recommend to MSLA possible measures for the mitigation of the vulnerabilities that were previously identified and documented.

- Verify that the measures implemented by MSLA have adequately addressed the reported vulnerabilities.

1.2 Lead Time

At this stage, the execution period was from December 18 to December 20, 2024.

1.3 Scope

The Scoping was carried out based on the stages described below:

- Starter joint. The personnel involved in carrying out the audit were summoned in order to present the activities considered as part of the audit, define the roles and responsibilities of the parties, establish the methodology and standards with which the audit will be carried out, as well as the general execution times.
- MSLA submitted a list of assets to the auditor for consideration during the kick-off meeting.
- MSLA provided workspaces to the members of the auditing body for the analysis of vulnerabilities to the technological infrastructure of the system.
- MSLA granted the corresponding accesses and the necessary time windows for the execution of the audit.

Detailed work plan. Based on the information obtained and analyzed, we prepared a detailed work plan for the security audit project of the MSLA technological infrastructure. This document will include the following:

- Penetration testing (pentest).
- Review of security configurations.

Penetration testing (pentest).

Penetration testing is performed both from inside and outside the data network to be examined and focused on:

- Servers.
- Web applications.
- Telecommunications equipment
- Workstations.

Revision of configurations.

The objective is to analyze the configurations of the devices that make up the technological infrastructure based on best computer security practices to identify opportunities and issue recommendations aimed at strengthening the security of equipment and information.

1.4 Methodology

The analysis and evaluation were carried out from 2 different points, with the first phase being an attack from outside and without knowledge of the network and the second was from within the network. Based on the methodologies known as ISSAF; OSWAP and the expertise of our experts.

2. PENETRATION TESTING AND CONFIGURATION REVIEW

2.1 Introduction

Penetration testing, also called "pen testing", is part of a technique used in the context of computer security to test a computer system in order to find vulnerabilities that a malicious attacker could use (exploit) for certain purposes. Ethical Hacking techniques and tools actively seek to exploit security vulnerabilities to obtain relevant information, just as an intruder would attempt.

Penetration testing can also be used to validate an organization's compliance with security policies, as well as its ability to identify and deal with computer security incidents and raise awareness among people who use computing devices.

The following report presents the results of the penetration tests carried out on the technological infrastructure, including the different devices present in the infrastructure that are key to carry out the Technical Operational Process of the MSLA system. Penetration testing was carried out from both inside and outside the data network to be examined and the following infrastructure was considered:

- Web Applications
- Telecommunications Equipment
- Workstations

The penetration tests carried out on the technological infrastructure are presented. The tests cover the different devices present in the infrastructure and that are key to carrying out the Technical Operational Process of MSLA's system.

2.2 Methodology.

The ***Issaf*** methodology for penetration testing is designed to evaluate the network, systems, and application of controls. They consist of three phases:

- Phase - I: Planning and preparation.
- Phase - II: Evaluation.
- Phase - III: Reporting.

PHASE - I: PLANNING AND PREPARATION:

This phase comprises the steps for initial information sharing, planning, and preparing for the test. The following activities are planned:

- Identification of contact persons on both sides.
- Kick-off ***meeting*** to confirm scope, approach and methodology.

PHASE - II: EVALUATION:

This is the phase where they actually conduct the penetration test. A layered approach is applied in the assessment phase, as shown below, each layer represents a higher level of access to your information assets.

2.3 Collection of Information

Information gathering is essentially the use of the Internet to find as much information as possible about the target (company or person) using both techniques (***DNS/WHOIS***, search engines, newsgroups, mailing lists, etc.). When performing any type of test on an information system, mining information and data collection is essential and provides as much information as possible to continue with the evaluation. It attempts to explore in every possible avenue to gain more understanding of its destiny and resources. Anything you can get your hands on at this stage of the test is useful: brochures, cards, newspaper ads, internal documents, and so on.

2.4 Mapping of the network and/or systems

After the first section, when as much information as possible about the target has been acquired, a more technical approach known as the "fingerprint" of the network" and the resources in question. The specific network information from the previous section is taken and expanded to produce a network topology. Many tools and applications can be used at this stage to aid the discovery of technical information about the hosts and networks participating in the test.

- Find the ***live hosts.***
- Port sweeping.
- Network assignment perimeter ***(router, firewall,*** etc.).
- Identification of critical services.
- Operating system ***(fingerprint).***

2.5 Identifying Vulnerabilities

Before starting this section, the auditor selects the specific points of the test and the manner of testing. During the identification of the vulnerability, the assessor will perform several activities for the detection of exploitation of the weak points.

These activities include:

- Identify vulnerable services using service banners.
- Perform vulnerability scans to look for known vulnerabilities. Information regarding known vulnerabilities can be obtained from vendor security announcements, or from public databases, such as ***SecurityFocus, nessus, CVE, or*** CERT ***advisories***, etc.
- Perform false positive and false negative verification (e.g., by correlating vulnerabilities with each other and with previously acquired information).
- List the vulnerabilities discovered.
- Estimate the likely impact (classification of vulnerabilities found).

2.6 Penetration

In this section, the objective is the same as the entire chapter:

"The evaluator tries to gain unauthorized access by circumventing security measures and tries to get to the highest level of access as possible."

2.7 Gain access and privilege escalation

In any given situation, a system can be listed further. The activities in this section will allow assessors to confirm and document the likely intrusion and/or spread of automated attacks. This allows for a better assessment of the impact for the organization as a whole.
Gain privileged access by gaining access to accounts through a variety of means, including:

- Discovery of username/password combinations (e.g., dictionary attacks, "*brute force" attacks*).
- Discovery of blank password or default passwords in the account system.
- Exploit default vendor settings (such as network configuration parameters, passwords, and others).

2.8 Enumerate

Obtain encrypted passwords (e.g., by dumping the ***SAM*** on Windows systems, or copying ***/etc/passwd and /etc/shadow from a Linux system***)

- Obtain the password (clear text or cipher) through ***snnifing*** or other techniques.
- The ***traffic snnif*** and analyze it.
- Collect ***cookies*** and use them to exploit sessions and password attacks.

2.9 Engage Remote Users/Sites

"A single hole is enough to expose the entire network," regardless of the perimeter network securement. Any system is only as strong as the weakest of its parts.
Communications between remote users, sites, and organizational networks should always be authenticated and encrypted, such as ***VPNs***, to ensure that data transiting the network cannot be eavesdropped, however, this does not guarantee that the communication endpoints have not been compromised (e.g.), the endpoints of the communication.

2.10 Maintaining Access

The use of covered channels ***(VPNs),*** exploitation of ***back-doors, rootkits*** allow gaining access to key applications or computers on the network.

2.11 Report of Findings

The findings found in the evaluations are reported in this document and in a final document.

2.12 Purpose of the section

The evaluator tries to gain unauthorized access by circumventing security measures and tries to reach the highest level of access as possible.

2.13 Procedure

Penetration tests to the technological platform were carried out using the following tools: Nessus, Owasp Zap, Acunetixs, Zenmap and Armitage as well as the Linux operating system distribution called Kali, as well as various tools and commands provided by the operating system. All the tools used were installed and used from the audit body's own equipment, which only required a direct connection to the communications equipment of the network to be analyzed to carry out the tests.

The tools used make it possible to execute all the tasks necessary to perform a reliable and reproducible vulnerability analysis of the technological infrastructure, as well as to exploit the vulnerabilities identified in the process in order to verify the risk level of the vulnerabilities discovered.

The analysis was divided into 3 phases:

1. Extraction and collection of information.
2. Port scanning and service identification.
3. Finding and exploiting vulnerabilities.

2.14 Extraction and collection of information.

Network probing serves as the analyst's basic knowledge of the devices to be analyzed. It can be defined as a combination of data collection, information gathering, and control policy. The objective is to build a map of the network with all the components that make up the technological platform, seeking to obtain as much information as possible for each device.

Expected results:

- Domain Names.
- Server Names.
- IP addresses.
- Network Map.

Methodology:

1. Find segments of used IPs through discovery tools.
2. Identify the network interface used by the devices.
3. Perform a reverse name identification from the identified IP addresses.

Tests Executed:

Poll with Zenmap to the networks and segments that were accessed. nmap -T4 -A -v to the networks and segments that were accessed.

2.15 Port Scanning & Service Identification

This test lists the active or accessible ports and services of each device that makes up the MSLA´s technology platform. The analysis of ports and services was carried out based on the type of device and the services offered by it. Once the services have been identified, an attempt will be made to identify the type of device, its operating system, version, and service packs or update version.

Expected results:

- Open, closed, and filtered ports.
- Internal IP addresses of active devices.
- List of discovered protocols.
- Active services.
- Type of Operating System.
- Service Pack or updates (security patches) installed.

Methodology:

1. Collect broadcast responses from the network.
2. Use scans to list open, closed, or filtered ports, for those TCP and UDP ports used by default on all computers on the network.
3. Relate each open port to a service and protocol.
4. Identify the level of updating (security patches) of the system.

Tests Executed:

- Analysis with nmap.
- Analysis with the Nessus tool.
- Analysis with acunetix tool.
- Analysis with Armitage tool.
- Analysis with Owasp Zap.
- Analysis with Kali Linux Tools.
- Analysis with Operating System commands.
- Analysis with Aqunetix Software.

2.16 Finding and exploiting vulnerabilities.

The purpose of this test is to identify, understand, and verify weaknesses, misconfigurations, and vulnerabilities in a device in the vendor's technology infrastructure. Finding vulnerabilities using automated tools is an efficient way to determine existing security issues as well as the level of up-to-date systems. On the other hand, the exploitation of vulnerabilities is carried out in order to corroborate whether it is possible to use externally the weaknesses found in order to take control or cause significant damage to the devices of the provider's technological infrastructure or in the operational process.

Expected results:

- Type of application or service by vulnerability.
- Update levels (security patches) of systems and applications.
- List of possible denial-of-service vulnerabilities.
- List of current vulnerabilities.
- List of internal systems.

Methodology:

- Integrate the scanners, hacking tools and exploits currently used (ethical-hacking) into the tests carried out.
- Measure the target network using current scanning tools.
- Attempt to determine vulnerabilities by application type and system
- Attempt to adjust vulnerabilities to services.
- Identify all application-related vulnerabilities.
- Identify all vulnerabilities related to operating systems to target systems.
- Check all vulnerabilities found during the exploit hunting phase.

Tests Executed:

- Additional vulnerability identification using Armitage.
- Exploiting vulnerabilities using Armitage.

3. FINDINGS

3.1 Revision of configurations

To date, the tests were carried out where it was possible to observe the results shown:

3.1.1 Live Host and open ports in the analyzed segments.

- 20 live hosts were found; Each one was analyzed and the necessary measures were taken for their safety.
- The ports that are open are listed for each computer. The need for each open port is analyzed together with those responsible and those that must be kept open are protected.

3.2 Vulnerabilities found.

Any vulnerability creates breaches in the integrity of the network or software, which attackers can exploit to gain access. Once inside, an attacker can perform malicious attacks, steal sensitive data, and cause major damage to critical systems. This report provides a summary of the vulnerabilities found.

4. REVIEW OF CONFIGURATIONS, ELECTRICAL CONDITIONS AND INTERNET SERVICES

4.1 Introduction

Adequate physical and environmental security ensures the availability of hardware and software systems, as well as other vital elements such as electrical power service, internal temperature, and internal temperature. This also ensures that the right environment is maintained for optimal performance and operation of the systems.

4.2 Objectives

Identify security weaknesses in the technological infrastructure by carrying out infrastructure tests in terms of redundancy to failures in the electrical power supply ranging from UPS (uninterruptible power supply) to tests with the current generator. In addition to the redundancy in internet services.

4.3 Lead Time

At this stage, the execution period was extended from December 18 to 20 and from December 26 to 28, 2024.

4.4 Scope

The tests performed are:

- Internet Failover Testing (Failover of Internet Service by Provider)
- Electrical failover tests to verify the performance of UPS (Uninterruptible Power Supply)
- Supply failover tests in the secondary CCV. With electric power plant.
- The procedure used by the staff of the area visited, as well as the secondary and primary CVCs, was observed and verified in detail.

4.5 Methodology

The tests carried out were based on the methodologies known as ISSAF, in addition to the experience of our experts.

For internet failover tests (failover in the internet service by the provider) the cable that transports the internet service was disconnected.

The specific points of review were as follows:

- Emergency lighting.
- Electric Power Generator (Power Plant).
- UPS (Interrupted Power Supply Unit).
- Extension cord long enough to place the generator outdoors if it needs to be used.
- Protocol for restoring electrical power through the generator.
- Protocol for the restoration of power supply through the service provider (Luz del Sur).
- Security in physical access to MSLA equipment.
- Logical security in MSLA equipment.
- Adequate conditions of ventilation, humidity, etc.
- Existing video surveillance equipment in place.

4.6 Tests

4.6.1. Internet failover testing (failover of internet service by the provider).

Expected results:

- The secondary service must be switched (Make the switch) to automatic.
- The operability of applications should not be affected (it should be transparent to users).
- In case of return of the signal from the primary internet provider, the operability of applications should not be affected (it should be transparent to users).

Methodology:

- Disconnect the cable that carries the primary internet service from the receiving equipment.
- Reconnect the cable that carries the primary internet service to the receiving computer.

Results:

Primary CCV

By means of the tests described above, the failure of the internet service was caused during the 2nd. drill with the following results:

- The secondary service went into automatic.
- The operability of applications did not affect (it was transparent for users).
- With the return of the signal from the primary internet provider, the operability of applications was affected (it was transparent for users).

Secondary CCV

- The secondary service went into automatic.
- The operability of applications did not affect (it was transparent for users).
- With the return of the signal from the primary internet provider, the operability of applications was affected (it was transparent for users).

4.6.2. **Electrical failover** tests to verify the performance of the UPS (Uninterruptible Power Supply Unit).

Expected results:

- The UPS equipment must be switched (Switch) to automatic.
- The operability of applications should not be affected (it should be transparent to users).
- In the event of a return of electricity from the supplier, the operability of applications must not be affected (it must be transparent to users).

Methodology:

- Disconnect from the equipment from electrical power.
- Reconnect the computer to power.

Results

Primary CCV

By means of the tests described above, a failure in the power supply was caused in the 2nd. drill with the following results:

- The UPS equipment went into automatic.
- The operability of applications was not affected (it was transparent for users)
- With the return of the signal from the primary internet provider, the operability of applications was affected (it was transparent for users).

Secondary CCV

- The secondary service went into automatic.
- The operability of applications did not affect (it was transparent for users).
- With the return of the power supply service, the operability of applications was not affected (it was transparent for users).

Physical and Environmental Security

Description	Existence	Operation
Emergency lightning	Ok	Ok
Electric Power Generator (Power Plant)	Ok	Ok
UPS (Power Interrupted Unit)	Ok	Ok
Extension cord long enough to place the generator outdoors if it needs to be used	Ok	Ok
Protocol for restoring electrical power through the generator	Ok	Ok
Protocol for the restoration of power supply through the service provider.	Ok	Ok
Security in physical access to MSLA equipment	Ok	Ok
Logical security in MSLA equipment	Ok	Ok
Adequate conditions of ventilation, humidity, etc.	Ok	Ok
Existing video surveillance equipment in place	Ok	Ok

5. SUMMARY OF FINDINGS

	Type of test	INFORMATIVE	LOW	MEDIUM	HIGH	CRITICAL
1	CONFIGURATION ANALYSIS	0	0	0	0	0
2	VULNERABILITIES	57	10	13	1	0

All findings were addressed. Some were defined as false positives, the rest corrected.