# CSIRT Service Description

# Contents

## Security and intellectual property

| | |
|---|---|
| **CLASSIFICATION** | **Confidential** |
| **AREA** | **Security Assessment Services** |
| **AUTHOR** | **OneseQ** |
| **DATE OF CREATION** | **17/01/2022** |

# 1. Vulnerability assessment

- Objective: To analyse and understand confirmed vulnerabilities.
- Definition:

  The vulnerability assessment service consists of functions designed to understand vulnerability and its possible repercussions, identify the problem or underlying fault (root cause) which enables a vulnerability to be exploited, and determine one or more repair or mitigation strategies to avoid the vulnerability being exploited or reduce this exploitation to a minimum.

OneseQ advocates for all our clients having secure work environments, as well as guidelines on improvement which will ensure a permanent state of security and calm, by guaranteeing the integrity, security and availability of all the items of value which are made up of their assets, in any unwanted situation.

Given the impact that any vulnerability has on our clients' business development, it is deemed appropriate to carry out assessment through cyber exercises to measure the degree of exposure to risk and vulnerabilities, evaluate the status of security measures and checks implemented and contribute suitable improvements and solutions for each vulnerability detected during this process.

In this way, it is ensured that work can be done efficiently and independently, with the confidence that the security and availability of the infrastructures and services exposed are permanently guaranteed or, in the worst case, that a rapid response can be provided to events that pose a risk to the continuity of our clients' businesses.

OneseQ proposes automated vulnerability scans, with evaluation and analysis of the results providing the recommendations for measures to consider and the security checks that will mitigate the deficiencies located.

By using vulnerability scan tests and analysis of the degree of exposure to risk, the aim is to:

- Identify vulnerabilities in order to be able to mitigate the risks associated with them.
- Establish the real, applicable mechanisms necessary to correct the vulnerabilities detected in the analysis performed.
- Perform other kinds of penetration testing which may be applicable according to the results of the vulnerability scan and the experience of the OneseQ team.

## 1.1. Step 1: Analysis and collection of information

This consists of collecting as much information about the systems as possible by carrying out an analysis of the environment with the support of the different tools that serve this purpose.

So, a search will be performed of domain names, IP addresses, possible user names, public databases, etc.

An analysis will be carried out of the target systems in order to identify active services, available machines, network mapping, operating systems and any configuration item which we are going to scan for vulnerabilities.

## 1.2. Step 2: Vulnerability scan

Automated tests and scans are run to identify specific resources and particular characteristics. A search is made of the versions of the operating systems and services, security patches and valid user accounts. We try to locate the possible and potential vulnerabilities, both in the system architecture and the system itself.

## 1.3. Step 3: Exploitation

This is a set of techniques for performing a complete evaluation of the weaknesses detected in the supported platforms. This model will reproduce attempts to gain access to web services and perimeter services, by simulating a potential penetration remotely.

It will enable the detection of the potential vulnerability and the weak points in security of the architecture supporting the applications relating to the exposed services.

It allows us to define other, secondary targets to run through scans that are aimed at other technological services or systems.

Exercises to check vulnerabilities will be run manually by the specialist technical team. Exploitation and execution will not be carried out unless they have been authorised.

## 1.4. Step 4: Report generation

This stage is considered to be the most important part of the assessment and it is here that a report will be made on each of the actions and tests that have been performed. It includes a description of the techniques and tools used in carrying out the tests, as well as the vulnerabilities found and the degree of severity that these present.

The deliverables are prepared, which should at least include the following:

- Technical reports
    - Map of the current security architecture
    - Proposed map to improve the security architecture
    - Security regulations and good practices
- Executive summary
- Security Recommendations:
    - Technological recommendations on protection and defence
    - Recommendations regarding solutions and services

## 2. Work methodology

| INFORMATION GATHERING 1 | ANALYSIS 2 | DIAGNOSIS 3 | DEPLOYMENT 4 | AUDIT 5 |
|---|---|---|---|---|
| Gathering of data and information relating to the project. | Analysis of information and asset simplification in domains. | Contact made directly with resources participating in the project. | Preparation of Gantt chart, Deployment Plan and Work Team. | VAK® cyber exercise on the Network and Ethical Hacking to determine level of protection. |
| Preparation of case examples and inventory of CIs, solutions and systems. | Analysis of optimisation initiatives regarding the Current model of ITC security. | Preparation of case examples and QA on solutions and/or validated services. | Implementation of the Solutions and Services approved. | Calculation of the technical benefit obtained through these solutions. |
| Preparation of the current Model Map of the Security Architecture. | Preparation of the Model Map of the new Security Architecture. | Design of the real current Model versus the vision of the future. | Status Reports on the progress of implementation. | Security Audit Reports. |
| Preparation of the inventory of CIs, of the Security Architecture. | Prioritisation of security solutions, services or initiatives. | Directed analysis of the Cyber Laboratory results. | Progress to production of Implemented Solution and Services. Solution End. | Preparation of cases of Continuous Improvement and/or new services. |

The methodology used by OneseQ is based on the OSSTMM (Open Source Security Testing Methodology) model and the OWASP which comply with the LOPD (*Protection of Personal Data Act*) and the ISO 17799/27000 standard, among others, whereby an exhaustive analysis is performed, not only regarding vulnerabilities but also procedures and courses of action.

- **Penetration Test**: automated external security analysis run by the SOC in search of vulnerabilities in services in terms of the internet and configuration faults in applications/web services, servers, routers, comms and firewalls, etc.
- **Internal Analysis**: evaluation of the application's internal security in search of vulnerabilities relating to services and configuration faults in the range of applications/web services.

The handling of project management processes will continue to be under ITILv3 methodology to ensure project standardisation and quality.

## 3. Management system

The specialist technician's work method will observe the following stages:

- Definition of Scope and Objectives for the Penetration Test cyber exercise on the system being examined in order to detect possible vulnerabilities
- Initial study of the environment to be evaluated
- Identification of the characteristics and granularity to be applied to the penetration test cyber exercise.
- Preparation of the cyber exercise plan and outlines.
- Automated, planned activities that are appropriate for the penetration test cyber exercise

Preparation of the final deliverables for the project.

## 4. Security principles

It must be decided how to rate the estimated risk level (High/Moderate/Low/Acceptable) which will be used as the parameter to classify vulnerabilities.

- Only one attack tool will be used per test target, to avoid or minimise accidental exploitation of vulnerabilities which will have an impact on the capacity and/or availability of the technological platforms or connected devices.
- The same test or stage can be run on the Target Servers more than once, but with different tools, for the purposes of comparison and optimisation of results.
- A register and documentation of evidence and identified vulnerabilities should be kept for each target in the cyber exercise.
- Vulnerability assessments should be conducted with complete consent and approval from the change control board to avoid server crashes or faults, inactive cycles or any other incident caused inadvertently by scanning activities. For this reason, the automated cyber exercise should previously determine what is required to run the tests in a controlled environment.
- For no reason and under no circumstances is any member of the work team authorised to disclose information obtained from conducting the exercises.
- The cyber exercises should ensure compliance with the CLIENT'S existing management policy, their procedures, instructions and manuals.
- The automated cyber exercise should be directly and constantly linked to the running of the project target, in accordance with the plan of characteristics and workloads, during the procedure and execution of each scenario within the cyber exercise.
- The work team should include at least one person from the CLIENT, with a position and profile of suitable authority to be able to overcome any setbacks in the phases of meeting test requirements. Only a Project Manager and a specialist are needed for the tests involved in the vulnerability scan cyber exercise.

## 5. Context of the cyber exercise

Each scenario should unfold following the stages established in the work plan and with all the documentation presented correctly in accordance with the schedule for deliverables.

OneseQ and the CLIENT will adjust the start and end dates for each of the activities contained in the work plan and will also establish the criteria for monitoring and control of the expected results.

As the first stage of the project, OneseQ and the CLIENT should carry out risk identification and evaluation regarding the performance of vulnerability assessments, which should contain the following information at least:

- Description of the Activity
- Threat
- Vulnerability
- Risk Description
- Probability of Occurrence
- Impact
- Risk level
- Recommendations and/or mitigating activities

In this stage, in order to run the second scenario of tests and analysis of the degree of exposure to risk, the information collected and generated by the first scenario should be used to make a comparison of the status of risk identification and evaluation.

For tests on information assets, only the IP addresses and the related services are needed.

Depending on the information obtained during the collection of information, the specialist will establish the tool or tools necessary for the running of vulnerability scans.

For each cycle of vulnerability assessment that is conducted and finished, the specialist will provide an executive summary which will contain the following elements at least:

- Description of the tests conducted.
- Methodology used.
- List of vulnerabilities found in the items on the technological platform.
- Ports and services enabled.
- Evidence of the information to which access was gained in the device.
- Actions which could be performed.
- Identification of threats to the information (Loss, Modification, Leakage or other).
- Possible solution or recommendation, that is realistic and executable, to correct the vulnerabilities, indicating the actions to be taken.

In this stage, to run the second scenario of tests, the information collected and generated by the first scenario should be used to make a comparison of the vulnerability assessments.

## 6. Requirements

To perform this service, a letter of authorisation will be needed to be able to conduct the tests involved in the penetration test; a confidentiality agreement will be drawn up as an annex to the approval of the work plan. Additionally, all the tests should be documented and outlined in writing beforehand, so that both parties concerned are in agreement.

As a result of the penetration test, a descriptive report will be produced on the current status of vulnerabilities that are external to the systems tested. It will include all the activities performed, the vulnerabilities and security problems detected, and the recommendations on solutions to be implemented to correct them.

In the case of the internal audit, the audit team should be granted access via VPN, for the operating systems Linux and Windows, and support will be provided for any incident relating to the VPN connection and other internal unforeseen events which may occur in relation to network routing. Routing is a key point, as it should directly reach all the assets included in the scope of the project, without interference from the IPS/IDS, unless this is expressly requested, which will modify the cost and effort required.

All the data, credentials and technology requested must be provided, as well as network mapping which makes it possible for all the requested assets to be perfectly audited.

A technical contact should be provided, who will give support to the correct running of the exercise at all times.

# 7. Tests:

## 7.1. Service tests

- Automatic Vulnerability Scan
- Measurement of the target organisation against popular scanning tools.
- Identification of system vulnerabilities by types of service.
- Attempt to match vulnerabilities to applications.
- Attempt to determine the type of application and service by vulnerability.
- Running a redundant test with at least two automated vulnerability scanners.

Analysis of the information obtained using automated technologies and tools.

- Identification of all vulnerabilities according to the operating systems.
- Identification of all vulnerabilities in similar systems which may also affect the target systems.
- Verification and manual checking of vulnerabilities.
- Verification of all the vulnerabilities found during the running of the exploit stage in search of false positives.
- Verification of all the high and critical positives.
- Verification of the robustness and security of SSL services.
- Performing brute-force attacks on the platforms that enable this.
- Analysis of network traffic in search of anomalies.
- Detailed description of the process of preparation and presentation of the final audit report.

The functioning of the cyber exercise will take shape in writing exclusively. Therefore, the final report is the exponent of its quality and the result of all the operations performed.

In developing this stage, the specialist and the project manager will perform an analysis of the results obtained in order to determine whether the effects of the tests conducted have met the desired objective. Depending on this evaluation, the specialist may reprogramme any tests that are necessary, following agreement with the CLIENT, and will later prepare the reports and corresponding presentation.

## 8. Deliverables

These tests in the vulnerability scan will provide the ICT security department with the following deliverables:

- Technical report on vulnerabilities prepared through automated identification of weaknesses caused by incorrect configuration of applications.
- Analysis and classification of the weaknesses exploited by the OneseQ SOC machines, based on the potential impact and the possibility of the threat becoming a reality.
- Recommendations based on the priorities established to mitigate and remove vulnerabilities and thereby reduce the risk of any unfavourable event occurring.
- Executive summary of the project aimed at top management.

OneseQ will hand over the report, both in digital format and in print, together with the scanned report, when it has been signed, or in formats that are compatible with document visualisation tools.

At the end of the two scenarios in the vulnerability scan tests and the analysis of the degree of exposure to risk, the project manager will draw up the project closure report and terminate the cyber exercise.

For each test cycle that is completed and at the specific request of the supervisor of the assigned project, the specialist may provide a partial report on results which will contain the following elements at least:

- Description of the work performed
- Summary of the activities conducted
- Description of the main findings
- Conclusions
- Recommendations