${project\_name}

${client\_name}

www.talsoft.com.ar

c

Ethical Hacking Report

Document details

|  |  |
| --- | --- |
| **Document Type** | ${document\_type} |
| **Document Version** | ${document\_ver} |
| **Clasification** | Confidencial |

Client details

|  |  |
| --- | --- |
| **Company** | ${client\_name} |
| **Address** | ${client\_address} |
| **City** | ${client\_city} |
| **Contact** | ${client\_contact} |

Version history

|  |  |  |
| --- | --- | --- |
| **Version** | Date | Authors |
| ${ver} | ${ver\_date} | ${ver\_testers} |

Business Summary

**${client\_name}** xxxxxx.

The testing times were made from  **${project\_initdate} hasta el día ${project\_enddate}**.

xxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxx.

The **biggest impact** problem **was ${risk\_higher}.**

The impact of the problems encountered are Medium and Low Risk because the various vulnerabilities **compromise the integrity, availability and confidentiality of the information.**

INITIAL Test Summary

|  |  |  |
| --- | --- | --- |
| High-Critical | Medium | Low |
| ${risk\_counthigh1} | ${risk\_countmed1} | ${risk\_countlow1} |

Detail of Risk

**${client\_name}** should continue to review its business security and perform **${project\_type}** tests at least twice a year, to have an acceptable level of security over time.

Listed below are the problems encountered:

Critical/High IMpact

|  |  |
| --- | --- |
| **${incidents\_listhigh}** |  |

Medium impact

|  |  |
| --- | --- |
| **${incidents\_listmed}** |  |

Technical specifications

The following tests were performed based on the size of the system:

${project\_metodology}

scope

The test was made over:

${project\_scope}

TOOLS

Xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

start and end testing

The following tests were performed based on the size of the system:

|  |  |
| --- | --- |
| Date | Description |
| ${date1} | Start of Audit |
| ${date2} | End of Audit |

Standard used

xxxxxxxxxxxxxxxxxxxx

The risk assessment of each vulnerability was found in the CVSSv2 risk calculation standard.

references

* <http://www.first.org/cvss/cvss-guide>

[r](mailto:consultas@talsoft.com.ar)isk levels

|  |  |  |
| --- | --- | --- |
| CVSSv2 | Symbol | Description |
| 9.0-10 |  | **Critical - Level 5:** Vulnerabilities that allow remote intruders with root access or remote management capability. With this level of vulnerability, intruders can compromise the entire host. This level includes vulnerabilities that provide intruders access to read and write files, remote execution of commands as root or administrator user. Presence of backdoors and trojans. |
| 7.0-8.9 |  | **High - Level 4:** vulnerabilities that allow intruders with remote access, not necessarily with root or administrator access. Intruders can partially access system files (for example, read access but not write). Vulnerabilities that expose sensitive information. |
| 4.0-6.9 |  | **Medium - Level 3:** vulnerabilities that allow intruders access to specific information stored in the system, including security settings. Vulnerabilities at this level can be potentially dangerous to the host by intruders. Examples of Level 3 vulnerabilities include file content disclosure, host file access, directory indexing, rule filter disclosure and security mechanisms, susceptible to DoS attacks, and unauthorized use of services such as mail relaying. |
| 1.0-3.9 |  | **Low - Level 2:** vulnerabilities that expose sensitive system information, such as service version. With this information, intruders can investigate potential attacks against the system. |
| 0-0.9 |  | **Info - Level 1:** vulnerabilities that expose information, such as open ports. |

Summary of problems

The following is a list of summarized problems sorted by criticality:

References

|  |  |
| --- | --- |
| State | Description |
| Resolve | Fixed vulnerabilities |
| Not Resolve | Not fixed vulnerabilities |
| Understood | Not fixed vulnerabilities but assume the risk |

${incidenttable}

|  |  |  |
| --- | --- | --- |
| ${incidenttable\_title} | | ${incidenttable\_image} |
| CVSSv2 | ${incidenttable\_cvss} | |
| Details | ${incidenttable\_detail} | |
| Recommendation | ${incidenttable\_recom} | |
| State | ${incidenttable\_state} | |
|  |  | |

Ips - ports and services

${hosttable}

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Host | | | ${hosttable\_host} | | | | |
| Port | State | Risk | | CVSSv2 | Service | Details | Accordance |
| ${hosttable\_ports}   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | ${hosttable\_ports\_port} | ${hosttable\_ports\_state} | ${hosttable\_ports\_risk} | ${hosttable\_ports\_cvss} | ${hosttable\_ports\_serv} | ${hosttable\_ports\_deta} | ${hosttable\_ports\_acc} | | | | | | | | |

Problems Detail

${incidentdetail}

${incidentdetail\_title}

Description

${incidentdetail\_description}

CVSSv2: ${incidentdetail\_cvss}

${incidentdetail\_detail}

RECOMMENDATION

${incidentdetail\_recom}

${incidentdetail\_recom2}

TraCing

|  |  |
| --- | --- |
| Date/State/User | Details |
| ${trackDate}  ${trackState}  ${trackUser} | ${trackDetail} |

${/incidentdetail}