**Test and audit report**

**Lidl**

Author(s) First name Family name

Bachelor’s thesis or Master’s thesis

Month Year (e.g. September 2015)

Name of Field (e.g. Technology, communication and transport)

Name of Degree Programme (e.g. Degree Programme in Logistics Engineering)

|  |  |  |
| --- | --- | --- |
| jamk_fi_tunnus_sininen | | **Description** |
| Author(s)  Last name, First name | Type of publication  Master’s thesis | Date Month Year |
| Language of publication: |
| Number of pages | Permission for web publication: x |
| Title of publication  **Title**  Possible subtitle | | |
| Degree programme | | |
| Supervisor(s)  Last name, First name | | |
| Assigned by | | |
| Abstract  When completing this form, start from this field, on the row under the instructions, so that the font size remains 11.  The basic structure of the abstract is as follows:   * background * task and objectives * implementation method * results * conclusions.   In other words, the abstract summarises the work that has been done – not the content of the report. If there is room, the content of the report may be briefly mentioned.  The entire space reserved for the abstract must be used.  The abstract should be written in the past tense and with a passive voice. The text must not refer to the thesis, i.e., the words ‘this thesis’ must not be used. | | |
| Keywords/tags ([subjects](https://janet.finna.fi/Search/Results?lookfor=asiasanastot&prefiltered=format_Database&SearchForm_submit=Find&retainFilters=0&filter%5b%5d=format%3A%220%2FDatabase%2F%22&lng=en-gb)) | | |
| Miscellaneous ([Confidential information](https://intra.jamk.fi/opiskelijat/student/thesis/Pages/publicity.aspx)) | | |

Table of Contents

[1 Introduction 1](#_Toc501481998)

[2 Scope of the test 1](#_Toc501481999)

[3 Audit activities 1](#_Toc501482000)

[4 Main findings 1](#_Toc501482001)

[5 Recommendations 1](#_Toc501482002)

[6 Technical Report 1](#_Toc501482003)

[6.1 Tooling 2](#_Toc501482004)

[6.2 Executed Test Cases 2](#_Toc501482005)

[6.3 Information Gathering 2](#_Toc501482006)

[6.4 Service Enumeration 3](#_Toc501482007)

[6.5 Vulnerability Summary TO BE DONE 4](#_Toc501482008)

[6.6 Vulnerability Details TO BE DONE 5](#_Toc501482009)

[1.1.1 Ability Server 2.34 FTP STOR Buffer Overflow 5](#_Toc501482010)

[1.1.2 **SQL Injection** 6](#_Toc501482011)

[2. Sample Report - Attachments 7](#_Toc501482012)

SUMMARY

Introduction

This report will be graded from a standpoint of correctness and fullness to all aspects of the homework. The purpose of this report is to ensure that the student has a full understanding of security testing methodologies as well as the technical knowledge to meet the objectives of the course YIIP3200.

Objective

The objective of this assessment is to perform an external (Homework1) and internal (Homework2) network security test against the LDIL corporate network. The auditor group is tasked with following methodical approach in obtaining access to the objective goals. This test simulates an actual network security test and how would one start from beginning to end, including the overall report.

Requirements

* Overall High-Level Summary and Recommendations (non-technical)
  + Introduction
  + Scope of the test
  + How tests were conducted (project plan or similar)
  + Main findings
  + Recommendations
* Technical Report
  + Walkthrough and detailed outline of steps taken and tools used
* Each finding with included information; screenshots, walkthrough, and sample code if applicable.
* Any additional items that were not included

Summary

This report contains results from the network security test towards KAPUTO OY’s public network. The focus of this test is to evaluate the network security, identify systems, and perform vulnerability analysis while reporting the findings back to KAPUTO OY.

How tests were conducted…

Main findings…

When performing the network security test, there were several alarming vulnerabilities that were identified on KAPUTO OY’s network.

Sample Report - Recommendations

YII14S1 security tester recommends…

TÄHÄN PÄÄTTYY ESIMERKKI RAPORTTI JA ALKAA MEIDÄN TUOTOS

# Introduction

This auditing report is a group exercise and it is part of the Auditing and Testing Technical Security course.

LDIL is a national e-tailing company that also has one physical retail store with a POS-system. LDIL business environment consists of information systems and different network domains. Target of this audit is LDIL's systems and networks.

# Scope of the audit

Everything?

Tätä rajattava…

# Audit activities

Three groups were created from group A auditing personnel and each group was assigned part of the LDIL networks to perform the audit.

# Main findings

Based on their auditing findings each subgroup presented main findings and summary of these findings is presented here.

# Recommendations

Fix update process to keep everything updated and fix firewall rules.

# Technical Report

YTC16S1 technical security testers are utilized to test and audit the LDIL corporate network thoroughly. Throughout the testing process, set of tools and preplanned test cases are planned - based on use cases given on LDIL business logic. The architecture of the LDIL is known as well as LDIL personnel are aware that audit and testing is performed to the corporate system. The testing type lies between crystal and grey-box combination - mainly testing the tester’s effectiveness and also the vulnerabilities on outdated system.

## Tooling

The following tools were used to conduct the security assessment. The tools are divided into information gathering, vulnerability scanning and also on web testing.

|  |  |
| --- | --- |
| Tool and version | |
| Nmap | 6.40 |
| Nessus | 5.9 |
| OpenVas |  |
| Burp Suite |  |

## Executed Test Cases

The following table contains a list of tests that were conducted during the test. This table does not contain any indication whether or not the test found any vulnerabilities. Detected vulnerabilities are listed in section XX.

Apart from the detailed test cases, also exploratory testing was applied by using Burp suite.

|  |  |
| --- | --- |
| Test Cases | |
| Executed tests provided by Nmap | Port and service enumeration scan. |
| Executed tests provided by Nessus | Vulnerability scan. |
| Executed tests provided by OpenVas | Vulnerability scan |
| Burp Suite | Web application testing, penetration testing |

## Information Gathering

The information gathering portion of a test focuses on identifying the scope of the vulnerability assessment. During this test, YII14S1 security tester was tasked with KAPUTO OY’s public network. The specific IP addresses were:

**KAPUTO OY’s public IP-address**

192.168.1.2

## Service Enumeration

Liitteeseen tämä kappale ja tähän jokin teksti

Tähän kappaleeseen laitetaan segmenteittäin löydetyt avoimet portit.

* MGMT,
* Warehouse &
* ws/staff
* Internal
* Branch
* DMZ

The service enumeration portion of a security test focuses on gathering information about what services are alive on a system or systems. This part provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives the tester needed information before performing the actual vulnerability assessment.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.1.2 | **TCP:** 21,80,443  **UDP:** 161 |

## Vulnerability Summary Olisiko yhteenveto segmenteittäin?

DMZ taulukko

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Network segment | Critical | High | Medium | Low | Info |
| 10.0.0. |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Target\_name | | | | | |
| Test Information | | | | | |
| Start time: | | 13th February 2015 13:00 | | | |
| End time: | | 13th February 2014 20:00 | | | |
| Host Information | | | | | | |
| DNS Name: | | www.kaputo.fi | | | |
| IP: | | 192.168.1.2 | | | |
| OS: | | Linux Debian 6.0 | | | |
| Open Ports: | | tcp/21 (FTP)  tcp/80 (HTTP) nginx 1.1.19 | | | |
|  | | tcp/443 (HTTPS) nginx 1.1.19 | | | |
|  | | udp/161 | | | |
| Results Summary | | | | | | |
| High | | Medium | Low | Info | Total |
| 2 | | 0 | 0 | 0 | 2 |
| Vulnerablities | | | | | | |
| 3.6.1 Ability Server 2.34 FTP STOR Buffer Overflow | | | | | | |
| Synopsis: | The remote service is vulnerable to buffer overflow vulnerability | | | | | |
| 3.6.2 SQL Injection | | | | | | |
| Synopsis: | The remote host is vulnerable to SQL injection | | | | | |
| High vulnerability (Vulnerability Title) | | | | | | |
| Synopsis: | Synopsis text. | | | | | |
| Medium vulnerability (Vulnerability Title) | | | | | | |
| Synopsis: | Synopsis text | | | | | |
| Low vulnerability (Vulnerability Title) | | | | | | |
| Synopsis: | Synopsis text | | | | | |
| Info (Info Title) | | | | | | |
| Synopsis: | Synopsis text. | | | | | |

## Vulnerability Details TO BE DONE

This section will give a more detailed information on each vulnerability. The details will cover explanation of the vulnerability, how it can be exploited if applicable, how the vulnerability can be mitigated or fixed, how severe the vulnerability is and additional information to help the reader to understand the vulnerability (e.q. screenshots, poc etc.).

|  |
| --- |
| Ability Server 2.34 FTP STOR Buffer Overflow **Synopsis:** The remote service is vulnerable to buffer overflow vulnerability  **Vulnerable Targets:** 192.168.1.2 tcp/21 (FTP)  **Vulnerability Explanation**: Ability Server 2.34 is subject to a buffer overflow vulnerability in STOR field. Attackers can use this vulnerability to cause arbitrary remote code execution and take completely control over the system.  **Vulnerability Fix**: The publishers of the Ability Server have issued a patch to fix this known issue. It can be found here: <http://www.code-crafters.com/abilityserver/>  **Severity: HIGH**  **References:** CVE-2014-0246  **CVSS Base Score:** X.X (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)  **Proof of Concept Code Here:**  N/A **Screenshot Here:**  N/A |

|  |  |  |
| --- | --- | --- |
| **SQL Injection** **Synopsis:** The remote host is vulnerable to SQL injection  **Vulnerable Targets:**   |  | | --- | | 192.168.1.2/welcome.php tcp/80 | | 192.168.1.2/welcome.php tcp/443 |   **Vulnerability Explanation**: A custom web application identified was prone to SQL Injection attacks. When performing the web application test, YII14S1 security tester noticed error-based MySQL Injection on the hello query string parameter. While enumerating table data, it was possible to successfully extract login and password credentials that were unencrypted that also matched username and password accounts for the root user account on the operating system. This allows for a successful breach of the Linux-based operating system as well as all data contained on the system.  **Vulnerability Fix**: Since this is a custom web application, a specific update will not properly solve this issue. The application will need to be programmed to properly sanitize user-input data, ensure that the user is running off of a limited user account, and that any sensitive data stored within the SQL database is properly encrypted. Custom error messages are highly recommended, as it becomes more challenging for the attacker to exploit a given weakness if errors are not being presented back to them.  **Severity: HIGH**  **References:** CVE-2014-4444  **Proof of Concept Code Here:**  SELECT \* FROM login WHERE id = 1 or 1=1 AND user LIKE "%root%" **Screenshot Here:**  N/A |

# Sample Report - Attachments

Include your attachments to the document. Typically the report is kept separate from technical scanner data and the attachments portion of the report contains additional information about the vulnerabilities, used test methods or policy guidelines that were followed during the testing.