**Information security audit report LDIL**

Group A

Bachelor’s thesis or Master’s thesis

January 2018

Technology, communication and transport

Cyber Security

|  |  |  |
| --- | --- | --- |
| 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](#_Toc503023660)

[2 Target organization 1](#_Toc503023661)

[3 Scope of the audit 1](#_Toc503023662)

[4 Audit activities 2](#_Toc503023663)

[4.1 Publicly available networks (DMZ, etc.) 2](#_Toc503023664)

[4.2 Workstation network and WEB testing (Internal and branch) 2](#_Toc503023665)

[4.3 Management networks (MGMT, warehouse and staff) 2](#_Toc503023666)

[5 Main findings 3](#_Toc503023667)

[5.1 Publicly available networks (DMZ, etc.) 3](#_Toc503023668)

[5.2 Workstation network (Internal and branch) 3](#_Toc503023669)

[5.3 Management networks (MGMT, warehouse and staff) 3](#_Toc503023670)

[6 Recommendations 3](#_Toc503023671)

[7 Detailed Technical Report 3](#_Toc503023672)

[7.1 Tooling 4](#_Toc503023673)

[7.2 Executed Test Cases 4](#_Toc503023674)

[7.3 Information Gathering 5](#_Toc503023675)

[7.4 Service Enumeration 5](#_Toc503023676)

[7.5 Vulnerability Summary Olisiko yhteenveto segmenteittäin? 5](#_Toc503023677)

[7.6 Vulnerability Details TO BE DONE 13](#_Toc503023678)

[1.1.1 Outdated jQuery library in use 13](#_Toc503023679)

[1.1.2 Outdated PHP version in use 13](#_Toc503023680)

[1.1.3 Verbose information about system version available in http response 14](#_Toc503023681)

[1.1.4 Verbose information about PHP and Apache version available in http response 14](#_Toc503023682)

[1.1.5 XSS-protection is not enabled 15](#_Toc503023683)

[1.1.6 Buffer overflow detected 16](#_Toc503023684)

[1.1.7 Directory browsing is enabled 16](#_Toc503023685)

[1.1.8 Format string error 17](#_Toc503023686)

[1.1.9 X-frame-options header not set 18](#_Toc503023687)

[1.1.10 MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution 18](#_Toc503023688)

[1.1.11 MS17-010: Security Update for Microsoft Windows SMB Server 19](#_Toc503023689)

[1.1.12 SSH Weak Algorithms Supported 20](#_Toc503023690)

[1.1.13 HTTP TRACE / TRACK Methods Allowed 20](#_Toc503023691)

[1.1.14 DNS Server Could Allow Remote Code Execution 21](#_Toc503023692)

[7.7 **Synopsis:** MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution 21](#_Toc503023693)

[7.8 **References:** CVE-2011-1966 21](#_Toc503023694)

[1.1.15 Security Update for Microsoft Windows SMB Server 22](#_Toc503023695)

[7.9 **Synopsis:** Security Update for Microsoft Windows SMB Server 22](#_Toc503023696)

[1.1.16 Vulnerability in Schannel Could Allow Remote Code Execution 23](#_Toc503023697)

[7.10 **Synopsis:** The remote Windows host is affected by a remote code execution vulnerability. 23](#_Toc503023698)

[1.1.17 Vulnerability in DNS Resolution Could Allow Remote Code Execution 24](#_Toc503023699)

[7.11 **Synopsis:** Arbitrary code can be executed on the remote host through the installed Windows DNS client. 24](#_Toc503023700)

[2. Sample Report - Attachments 25](#_Toc503023701)

# Introduction

This auditing report is a group exercise and it is part of the Auditing and Testing Technical Security course. Report includes external and internal network security tests performed against the LDIL corporate network. The goal of the technical security audit is to form overall picture relating to state of the security and offer recommendations for future improvements.

# Target organization

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 evaluation is LDIL's systems and networks related to customer and payment information.

# Scope of the audit

The reference framework used in this audit is Payment Card Industry Data Security Standard (PCI DSS). Based on this framework, all components that are part of cardholder data environment should be included to the scope of audit. Also, as assignment required, all other component that were available for testing were included. Even so, reference framework was required to transform priority rating for different systems to support audit priorities (findings, recommendations, etc.).

As a notice, it should be reminded that this audit is purely technical and do not include any administrative parts relating to used framework.

From technical perspective audit can also be divided to internal and external audit as presented below:

* **Internal audit** was performed inside LDIL’s network. Detailed information about network structure and host credentials were available for deep inspection.
* **External audit** was performed against LDIL’s publicly available network interface.

Detailed scope of technical functions (networks, etc.) is presented in next chapter.

# Audit activities

Three groups were created from group A auditing personnel and each group was assigned part of the LDIL network segments to perform the audit. The auditing groups were formed to most effectively utilize the assessor’s skills. Petri and Jouni were chosen as lead auditors to facilitate the auditing process.

Groups were following:

* Vesa & Pinja (Publicly available networks)
* Pauli, Jani, Otso & Janne (Workstation network and WEB testing)
* Jouni, Teemu & Petri (Management networks)

Network segments to be audited were divided based on workload estimates and logical entities.

Internal auditing activities were conducted by using virtualized Kali workstations and tools installed on them. These workstations had interfaces on all relevant network segments. External auditing activities were conducted by using RGCE internet workstation located outside of the LDIL network perimeter.

LDIL firewall rules (Palo Alto and pfsense) were reviewed to find possible shortcomings.

## Publicly available networks (DMZ, etc.)

Kertokaa omin sanoin mitä tehty

* Tools
* Short description of the network
  + Perustuu saatuun excel-listaukseen

## Workstation network and WEB testing (Internal and branch)

Kertokaa omin sanoin mitä tehty

## Management networks (MGMT, warehouse and staff)

Management networks auditing were conducted first by running a Nessus discovery scan to discover all connected hosts in the segments. Results from this scan were compared to the LDIL service catalog provided by LDIL personnel. After determining host’s operating systems and that no unrecognized hosts were not found, a new and more specific Nessus scans were conducted to acquire more information about the systems. Some findings were verified by using OpenVAS tool.

# Main findings

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

Firewall rule

* Yksi näkökulma: Verrattuna siihen olemassa olevaan dokumentaation (asiakkaan luovuttamaa)

## Publicly available networks (DMZ, etc.)

* Yleiskuvaus verkon tilasta

## Workstation network (Internal and branch)

## Management networks (MGMT, warehouse and staff)

Based on information gathered during the auditing activities most of the systems were poorly updated and therefore many security vulnerabilities were found.

# Recommendations

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

# Detailed Technical Report

Group A technical security testers were 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 listed in table 1 were used to conduct the security assessment. The tools are divided into information gathering, vulnerability scanning and also on web testing.

Table 1 Tools and versions used.

|  |  |
| --- | --- |
| Tools and version | |
| Nmap | 6.40 |
| Nessus | 5.9 |
| Openvas |  |
| Burp Suite |  |
| Owasp ZAP |  |

## Executed Test Cases

Table 2 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. Summary of detected vulnerabilities are listed in section 7.5.

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

Table 2 Executed test cases

|  |  |
| --- | --- |
| 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 / Owasp ZAP | 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. |  |  |  |  |  |

Table 3 Management networks vulnerabilities summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Network segment | Critical | High | Medium | Low | Info |
| 10.99.0.10 | 12 | 49 | 52 | 8 | 49 |
| 10.99.0.11 | 11 | 49 | 52 | 8 | 49 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File server (internal) | | | | | |
| Test Information | | | | | |
| Start time: | | 7th December 2017 18:00 | | | |
| End time: | | 7th December 2017 18:25 | | | |
| Host Information | | | | | | |
| DNS Name: | | files.ldil.de | | | |
| IP: | | 10.0.100.20 | | | |
| OS: | | Microsoft Windows Server 2008 R2 Standard Service Pack 1 | | | |
| Open Ports: | | tcp/135 ()  tcp/137 ()  udp/137 ()  tcp/139  tcp/445 (SMB) | | | |
|  | | udp/5355 (DNS LLMNR) | | | |
|  | | tcp/49152  tcp/49153  tcp/49154  tcp/49161  tcp/49177  tcp/62091 | | | |
| Results Summary | | | | | | |
| High | | Medium | Low | Info | Total |
| 2 | | 0 | 0 | **19** | 21 |
| Vulnerablities | | | | | | |
| 1.1.12 MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution | | | | | | |
| Synopsis: | Arbitrary code can be executed on the remote host through the installed Windows DNS client. | | | | | |
| 1.1.13 MS17-010: Security Update for Microsoft Windows SMB Server | | | | | | |
| Synopsis: | The remote Windows host is affected by multiple vulnerabilities. | | | | | |
| 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. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| POS (branch) | | | | | |
| Test Information | | | | | |
| Start time: | | 9th December 2017 13:09 | | | |
| End time: | | 9th December 2017 13:12 | | | |
| Host Information | | | | | | |
| DNS Name: | | pos.ldil.de | | | |
| IP: | | 192.168.10.20 | | | |
| OS: | | Linux Kernel 2.6 on CentOS Linux release 6 | | | |
| Open Ports: | | tcp/22 (SSH)  tcp/80 (http)  tcp/443 (https) | | | |
| Results Summary | | | | | | |
| High | | Medium | Low | Info | Total |
| 0 | | 3 | 2 | **31** | 36 |
| Vulnerablities | | | | | | |
| 1.1.14 Weak SSH algorithms supported | | | | | | |
| Synopsis: | The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all. | | | | | |
| 1.1.15 HTTP TRACE / TRACK Methods Allowed | | | | | | |
| Synopsis: | Debugging functions are enabled on the remote web server. | | | | | |
| SSH Server CBC Mode Ciphers Enabled | | | | | | |
| Synopsis: | The SSH server is configured to use Cipher Block Chaining. | | | | | |
| SSH Weak MAC Algorithms Enabled | | | | | | |
| Synopsis: | The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms. | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DC (Internal) | | | | | | |
| Test Information | | | | | | |
| Start time: | | 7th December 2017 19:00 | | | | |
| End time: | | 10th Decenmer 2017 20:00 | | | | |
| Host Information | | | | | | | |
| DNS Name: | | dc.ldil.de | | | | |
| IP: | | 10.0.100.10 | | | | |
| OS: | | Windows Server 2008 R2 ST SP1 | | | | |
| Open Ports: | | tcp/0  tcp/udp 53 DNS Microsoft DNS 6.1.760 | | | | |
|  | | tcp/88 Kerberos | | | | |
|  | | upd/123 NTP  tcp/135 DCE/RPC-service  udp/137 NetBIOS / SMB  tcp/139 SMB file / printer sharing  tcp/389 LDAP server  tcp/445 Windows SMB service  tcp/464 unknown  udp/500 IPSEC V2  tcp/593 http rpc epmap  tcp/636 LDAP server  tcp/3268 LDAP server  tcp/3269 LDAP server  tcp/3389 Windows Terminal Services  udp/5355 LLMN (Link-local Multicast Name Resolution)  tcp/5722 Unknown RPC service  tcp/49152 Unknown RPC service  tcp/49153 Event log TCPIP, NRP server endpoint, DHCPv6 Client LRPC Endpoint, DHCP Client LRPC Endpoint  tcp/49154 Several RPC services  tcp/49155 MS NT Directory DRS Interface, Local Security Authority, Security Account Manager, Network Logon Service  tcp/49158 Security Account Manager, Network Logon Service  tcp/49164 Service Control Manager  tcp/55034 DNS server  tcp/63180 DHCP server service | | | | |
| Results Summary | | | | | | | |
| High | | Medium | Low | Info | Total | |
| 4 | | 11 | 0 | 0 | 2 | |
| Vulnerablities | | | | | | | |
| 3.6.1 Vulnerabilities in DNS Server Could Allow Remote Code Execution | | | | | | | |
| Synopsis: | The DNS server running on the remote host has multiple vulnerabilities. | | | | | | |
| 3.6.2 Security Update for Microsoft Windows SMB Server | | | | | | | |
| Synopsis: | The remote Windows host is affected by multiple vulnerabilities | | | | | | |
| 3.6.3 Vulnerability in Schannel Could Allow Remote Code Execution | | | | | | | |
| Synopsis: | The remote Windows host is affected by a remote code execution vulnerability. | | | | | | |
| 3.6.4 Vulnerability in DNS Resolution Could Allow Remote Code Execution | | | | | | | |
| Synopsis: | Arbitrary code can be executed on the remote host through the installed Windows DNS client. | | | | | | |
|  |  | | | | | | |
| Medium  vulnerability IP Forwarding Enabled | | | | | | | |
| Synopsis: | The remote host has IP forwarding enabled | | | | | | |
| Vulnerability in DNS Server Could Allow Denial of Service | | | | | | | |
| Synopsis: | The DNS server running on the remote host is susceptible to a denial of service attack. | | | | | | |
| SSL Certificate Signed Using Weak Hashing Algorithm | | | | | | | |
| Synopsis: | An SSL certificate in the certificate chain has been signed using a weak hash algorithm. | | | | | | |
| SSL Medium Strength Cipher Suites Supported | | | | | | | |
| Synopsis: | The remote service supports the use of medium strength SSL ciphers. | | | | | | |
| SSL Certificate Cannot Be Trusted | | | | | | | |
| Synopsis: | The SSL certificate for this service cannot be trusted. | | | | | | |
| SSL Self-Signed Certificate | | | | | | | |
| Synopsis: | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. | | | | | | |
| TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE) | | | | | | | | Ting Oracle Information Disclosure Vulnerability (TLS POODLE) |
| Synopsis: | It was possible to obtain sensitive information from the remote host with TLS-enabled services. | | | | | | |
| SSL 64-bit Block Size Cipher Suites Supported (SWEET32) | | | | | | | |
| Synopsis: | The remote service supports the use of 64-bit block ciphers. | | | | | | |
| Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) | | | | | | | |
| The remote Windows host is affected by an elevation of privilege vulnerability. | | | | | |
| Medium vulnerability IP Forwarding Enabled | | | | | | | |
| The remote host has IP forwarding enabled | | | | | |
| Medium vulnerability IP Forwarding Enabled | | | | | | | |
| The remote host has IP forwarding enabled | | | | | |
|  |  | | | | | | |
|  |  | | | | | | |
|  |  | | | | | | |
| Low vulnerability (Vulnerability Title) | | | | | | | |
| Synopsis: | Synopsis text | | | | | | |
| Info (Info Title) | | | | | | | |
| Synopsis: | Synopsis text. | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RODC | | | | | |
| Test Information | | | | | |
| Start time: | | 7th December 2017 19:00 | | | |
| End time: | | 10th Decenmer 2017 20:00 | | | |
| Host Information | | | | | | |
| DNS Name: | | rodc.ldil.de | | | |
| IP: | | 192.168.10.10 | | | |
| OS: | | Microsoft Windows Server 2008 R2 Standard SP 1 | | | |
| Open Ports: | | tcp/0  udp/0  tcp/udp 53 DNS Microsoft DNS 6.1.760 | | | |
|  | | tcp/88 Kerberos | | | |
|  | | upd/123 NTP  tcp/135 DCE/RPC-service  udp/137 NetBIOS / SMB  tcp/139 SMB file / printer sharing  tcp/389 LDAP server  tcp/445 Windows SMB service  tcp/464 unknown  tcp/593 http rpc epmap  tcp/636 LDAP server  tcp/3268 LDAP server  tcp/3269 LDAP server  udp/5355 LLMN (Link-local Multicast Name Resolution)  tcp/5722 Unknown RPC service  tcp/49152 Unknown RPC service  tcp/49153 Event log TCPIP, NRP server endpoint, DHCPv6 Client LRPC Endpoint, DHCP Client LRPC Endpoint  tcp/49154 Several RPC services  tcp/49155 MS NT Directory DRS Interface, Local Security Authority, Security Account Manager, Network Logon Service  tcp/61238 DCE Services Enumeration  tcp/61272 DCE Services Enumeration  tcp/61279 DCE Services Enumeration | | | |
| Results Summary | | | | | | |
| High | | Medium | Low | Info | Total |
| 4 | | 11 | 0 | 0 | 2 |
| Vulnerablities | | | | | | |
| 3.6.1 Vulnerabilities in DNS Server Could Allow Remote Code Execution | | | | | | |
| Synopsis: | The DNS server running on the remote host has multiple vulnerabilities. | | | | | |
| 3.6.2 Security Update for Microsoft Windows SMB Server | | | | | | |
| Synopsis: | The remote Windows host is affected by multiple vulnerabilities | | | | | |
| 3.6.3 Vulnerability in Schannel Could Allow Remote Code Execution | | | | | | |
| Synopsis: | The remote Windows host is affected by a remote code execution vulnerability. | | | | | |
|  | | | | | | |
|  |  | | | | | |
|  |  | | | | | |
| Medium | | | | | | |
|  |  | | | | | |
| Vulnerability in DNS Server Could Allow Denial of Service | | | | | | |
| Synopsis: | The DNS server running on the remote host is susceptible to a denial of service attack. | | | | | |

## 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.).

### Outdated jQuery library in use

**Synopsis:** jQuery library is outdated and possibly vulnerable to exploits

**Vulnerable Targets:**

**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**: Update jQuery as well as the dependent libraries to the latest version.

**Severity: MEDIUM**

**References:** None

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### Outdated PHP version in use

**Synopsis:** PHP framework is outdated and possibly vulnerable to exploits

**Vulnerable Targets:**

**Vulnerability Explanation**: Intra-server is running unsupported PHP framework version, meaning there is no longer fixes and updates received from the PHP community.

**Vulnerability Fix**: Update PHP to at least to the one of the supported versions. Current version is not supported and might contain vulnerabilities as the support is no longer extended.

**Severity: MEDIUM**

**References:** None

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### Verbose information about system version available in http response

**Synopsis:** HTTP response includes information the operating system.

**Vulnerable Targets:** http://intra.ldil.de

**Vulnerability Explanation**: HTTP response gives out unneeded information to the end user and thus compromising the system security.

**Vulnerability Fix**: Hide the verbose response of currently used software versions from the http response.

**Severity: MEDIUM**

**References:** None

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### Verbose information about PHP and Apache version available in http response

**Synopsis:** Verbose information about the PHP and Apache versions present in http response.

**Vulnerable Targets:** http://intra.ldil.de

**Vulnerability Explanation**: Exposing the system version information to end-users is not needed. If it is needed internally, use different methods than printing it to http responses in plain-text (“Hi! I am using version..”).

**Vulnerability Fix**: Disable unneeded information sharing to end-users.

**Severity: MEDIUM**

**References:** None

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### XSS-protection is not enabled

**Synopsis:** Web browser XSS protection is not enabled or is disabled by the configuration of the X-XSS-Protection HTTP response header on the webserver.

**Vulnerable Targets:** http://intra.ldil.de

**Vulnerability Explanation**: The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser´s XSS protection mechanisms. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block.

The X-XSS-Protection HTTP response header is currently supported on IE, Chrome and Safari.

**Vulnerability Fix**: Ensure that the web browser´s XSS filter is enabled by setting the X-XSS-Protection HTTP response header to “1”.

**Severity: MINOR**

**References:** OWASP – Guidelines for setting security headers

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### Buffer overflow detected

**Synopsis:** Buffer overflow errors are happening when the overwriting of memory spaces of the background web process, which should never been modified intentionally or unintentionally. Overwriting values of the IP (instruction pointer), BP (base pointer) and other registers causes exceptions, segmentation faults and the other process errors to occur.

**Vulnerable Targets:** http://intra.ldil.de

**Vulnerability Explanation**: Potential buffer overflow detected. The script closed the connection and threw a 500 Internal Server Error.

**Vulnerability Fix**: Rewrite the background program using proper return length checking. This will require a recompile of the background executable.

**Severity: MEDIUM**

**References:** None

**Proof of Concept Code Here:**

GET

<https://intra.ldil.de/wp-content/themes/twentysixteen?query=xlScCqlemqpPtXbFamPILdDaLkKPaUyLMWHUlAa>...... Basically any long enough query  
**Screenshot Here:**

N/A

### Directory browsing is enabled

**Synopsis:** Directory browsing is enabled and it is possible to view the directory listing

**Vulnerable Targets:** https://intra.ldil.de/wp-admin

**Vulnerability Explanation**: It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files which can be accessed to read sensitive information.

**Vulnerability Fix**: Disable directory browsing. If the directory browsing cannot be disabled because of some other service needing it, make sure the listed files do not include any risks.

**Severity: MEDIUM**

**References:** Apache httpd - Options

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### Format string error

**Synopsis**: A format string error occurs when the submitted data of an input string is evaluated as a command by the application.

**Vulnerable Targets:** https://intra.ldil.de

**Vulnerability Explanation**: Potential format string error occurred. The script closed the connection on a /%s

**Vulnerability Fix**: Review the background program using proper deletion of bad character strings (parameterize). This will require a recompile of the background executable.

**Severity: MEDIUM**

**References:** https://www.owasp.org/index.php/Format\_string\_attack

**Proof of Concept Code Here:**

SAMPLE QUERY HERE QUERY  
**Screenshot Here:**

N/A

### X-frame-options header not set

**Synopsis:** X-Frame-Options header is not included in the HTTP response

**Vulnerable Targets:** http://intra.ldil.de

**Vulnerability Explanation**: X-Frame-Options header should be included in the HTTP response to protect against ClickJacking attacks.

**Vulnerability Fix**: Most modern web browsers support the X-Frame-Options HTTP header. Ensure it is set on all web pages returned to your site.

**Severity: MEDIUM**

**References:** MSDN – Combating clickjacking with x-frame-options

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution

**Synopsis:** Arbitrary code can be executed on the remote host through the installed Windows DNS client.

**Vulnerable Targets:** http://files.ldil.de

**Vulnerability Explanation**: A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to

execute arbitrary code in the context of the NetworkService account. On Windows Vista, 2008, 7, and 2008 R2, the issue can be exploited remotely.

**Vulnerability Fix**: Install patch for Windows 2008 R2.

**Severity: HIGH**

**References:** https://www.tenable.com/plugins/index.php?view=single&id=53514

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### MS17-010: Security Update for Microsoft Windows SMB Server

**Synopsis:** Multiple vulnerabilities in Microsoft Server Message Block 1.0 (SMBv1)

**Vulnerable Targets:** http://files.ldil.de

**Vulnerability Explanation**: Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. Exploiting vulnerability is possible for unauthenticated attacker via specially crafted packet, to achieve arbitrary code execution. Related vulnerabilities in National Vulnerability Database: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148.

Also, an information disclosure vulnerability exists in SMB. Exploiting vulnerability is possible for unauthenticated attacker via specially crafted packet, to disclose sensitive information. Related vulnerability in NVD: CVE-2017-0147

In addition, SMB vulnerabilities exist that are exploited by WannaCry/WannaCrypt ransomware, EternalRocks worm and Petya ransomware.

**Vulnerability Fix**: Install patch for Windows 2008 R2.

**Severity: HIGH**

**References:** https://www.tenable.com/plugins/index.php?view=single&id=97833

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### SSH Weak Algorithms Supported

**Synopsis:** The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

**Vulnerable Targets:** http://pos.ldil.de

**Vulnerability Explanation**: Remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

**Vulnerability Fix**: Configure SSH server to remove weak algorithm.

**Severity: MEDIUM**

**References:**

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

### HTTP TRACE / TRACK Methods Allowed

**Synopsis:** Debugging functions are enabled on the remote web server.

**Vulnerable Targets:** http://pos.ldil.de

**Vulnerability Explanation**: The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

**Vulnerability Fix**: Refer to Apache web server documentation on how to disable these methods.

**Severity: MEDIUM**

**References:**

**Proof of Concept Code Here:**

N/A  
**Screenshot Here:**

N/A

|  |
| --- |
| DNS Server Could Allow Remote Code Execution**Synopsis:** MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution **Vulnerable Targets:** 10.0.100.10 udp/53 (DNS)  **Vulnerability Explanation**: A remote code execution vulnerability exists in the way that the Windows DNS Server improperly handles a specially crafted NAPTR query string in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  **Vulnerability Fix**: Microsoft has released a set of patches for Windows 2003, 2008, and 2008 R2. <http://technet.microsoft.com/en-us/security/bulletin/ms11-058>  **Severity: HIGH** **References:** CVE-2011-1966 **CVSS Base Score:** 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)  **Proof of Concept Code Here:**  N/A **Screenshot Here:**  N/A |

|  |  |
| --- | --- |
| **Security Update for Microsoft Windows SMB Server****Synopsis:** Security Update for Microsoft Windows SMB Server **Vulnerable Targets:**   |  | | --- | | 10.0.100.10 445/tcp Microsoft Windows SMB service |   **Vulnerability Explanation**: The remote Windows host is affected by the following vulnerabilities :  - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)  - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)  **Vulnerability Fix**: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.  **Severity: HIGH**  **References:** CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148  **Proof of Concept Code Here:**  N/A **Screenshot Here:**  N/A |

|  |  |
| --- | --- |
| **Vulnerability in Schannel Could Allow Remote Code Execution****Synopsis:** The remote Windows host is affected by a remote code execution vulnerability. **Vulnerable Targets:**   |  | | --- | | 10.0.100.10 445/tcp Microsoft Windows SMB service |   **Vulnerability Explanation**: The remote Windows host is affected by the following vulnerabilities :  - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)  - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)  **Vulnerability Fix**: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.**Severity: HIGH**  **References:** CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148  **Proof of Concept Code Here:**  N/A **Screenshot Here:**  N/A |

|  |  |
| --- | --- |
| **Vulnerability in DNS Resolution Could Allow Remote Code Execution****Synopsis:** Arbitrary code can be executed on the remote host through the installed Windows DNS client. **Vulnerable Targets:**   |  | | --- | | 10.0.100.10 445/tcp Microsoft Windows SMB service |   **Vulnerability Explanation**: The remote Windows host is affected by the following vulnerabilities:  - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)  - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)  **Vulnerability Fix**: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.**Severity: HIGH**  **References:** CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148  **Proof of Concept Code Here:**  N/A **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.