jamk.fi

Information Security Audit Report LDIL.DE

Group A

Group Assignment
January 2018
Technology, communication and transport
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Jani Lindholm Otso Korpelainen Vesa Simola Pauli Paatsola Pinja Koskinen Petri Toropainen Teemu Hokkanen Jouni Ihanus Janne Ahokas Otso Korpela Jani Lindholm	Group Assignment	January 2018
		Language of publication:
	Number of pages	Permission for web publication: x

Title of publication

Group Assignment: Information Security Audit Report for LDIL.DE

Degree programme

Master's Degree Programme in Information Technology

Supervisor(s)

Lötjönen, Jarmo

Assigned by

Lötjönen, Jarmo

Abstract

This document presents information security audit report for LDIL.DE. Assignment is part of auditing and testing technical security course.

The main reference framework used in this audit is Payment Card Industry Data Security Standard (PCI DSS). Also, some part outside this framework is presented as required in assignment.

Document walks through accomplished audit activities and main findings, ending with recommendations and detailed technical report. Full reports produced by auditing tools are included as attachment.

Conclusion is that technical environment does not fully comply with PCI DSS. The management should take in to consideration findings presented in this document as part of the risk management activities. Recommendations should be prioritized and responsibilities should be defined.

Keywords/tags (subjects)

Security, Audit, NMAP, Nessus, OWASP

Miscellaneous (Confidential information)

Table of Contents

Figures

No table of figures entries found.

Tables

1 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.

2 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.

3 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 most of the 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.

4 Audit activities

Three subgroups 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 by 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 and RGCE Nessus service.

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

Used review techniques in this audit can be divided in two parts:

- Passive techniques
    - Documentation review
    - Ruleset review (Firewall)
- Active techniques
    - Network discovery
    - Network port and service identification
    - Vulnerability scanning

There were small differences in used techniques and activities based on what kind of functions were under inspection. These details are presented in next chapters.

4.1 Publicly available networks (DMZ, etc.)

Premilinary scanning of the public address space and 1:1 NAT inside network was performed using Nessus vulnerability scanner and Nmap port scanner. Two aforementioned tools were used from both inside and outside of the perimeter

firewall. First order of business was running Nmap and Nessus was used to both confirm the Nmap findings and to scan for higher level vulnerabilities. Reports produced by the automated scanners were analyzed manually to find the most relevant issues that were deemed worthy of escalation. Masses of bulk vulnerabilities that were found were intentionally left out as they could have been trivially patched assuming patches where available in RGCE. These are still reported in the attachments.

Hence, we selected a few of the more critical and subject-wise interesting vulnerabilities, for example: Shellshock and weak encryption mechanisms. These are discussed in more detail from the ldil.de perspective with PCI DSS angle.

4.2 Workstation network and WEB testing (Internal and branch)

Internal and Branch networks included the following network segments:

- Internal 10.0.100.1/24
- Branch 192.168.10.1/24

Web testing was conducted to corresponding web-services found in internal-branch-servers.
Focus of web testing was to discover application flaws or misconfigurations. Web testing revealed certain issues regarding the used libraries, operating system and applications. Verbose error http responses are spreading out too much information about the target machines, e.g. stating the version of PHP, OS and Apache.

Threats regarding the application were discovered by either manually testing or automatically scanning the target machines with Owasp ZAP and Nessus.

We were comparing the regarding the vulnerability scanning, by evaluating both Nessus and OpenVAS - but we ended up using Nessus because of company policy, other participants in the conducted audit were also using the Nessus.

More detailed issue reports can be found on chapter 7. In addition to verbose http responses or error messages, there were also buffer overflows, misconfigured application/server issues found.

4.3 Management networks (MGMT, warehouse and staff)

Management networks included the following network segments:

- MGMT 10.99.0.1/24
- Warehouse/Staff 172.20.0.0/24

From the PCI DSS point of view, especially MGMT-segment is critical. Most of the management devices are located in this network segment as well as log servers just to mention a few. In order to ensure the security of CPE environment, these can be seen as critical components.

Auditing were conducted first by running a Nessus discovery scan to discover all connected hosts in all 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.

5 Main findings

Based on auditing activities presented above, the most important findings are presented as follows. Priority is estimated against PCI DSS.

5.1 Segmentation

The PCI DSS audit criteria's scope contains everything that is involved in processing or transferring of cardholder data. Thus segmentation, on top of being a sound cyber security policy in its own right, directly affects which parts of the organizations network are also part of the cardholder data environment (CDE). Only the CDE has to be audited with the PCI DSS criteria.

First of all, the services that are not supposed to be accessible from the Internet are not facing Internet. Only the external ones, like email, web page and external name services are available. Everything else from the Internet to DMZ and to the rest of the Internal network of Ldil has been explicitly blocked.

Also, all the services that need to connect from one network segment to another have been separately defined so that network-wise they can only connect to their intended destinations. Also, all the undefined connections from the DMZ to other parts of the Ldil's network have been explicitly blocked.

Connectivity from different network segments inside Ldil's network has also been restricted to minimum, with down to nominating specific address' and applications when possible. Using the report Cyber Security Implementation (for the Ldil –store) it's not clear which parts or which computers belong to CDE. For example, the connection from the store Point Of Sale (POS) device is not defined. Also, the report doesn't make any remark about the settings of the firewall(s) at the branch stores.

5.2 Publicly available networks (DMZ, etc.)

General consensus is that the majority of the vulnerabilities found during our scanning of both the inside and outside address spaces of the 1:1 NAT were a result of missing software updates on the relevant servers.

Now, the reason for this most likely is that there simply was no updates available in the RGCE mirrors, hence we've decided to skip the low hanging fruits this scenario proposed and instead we attempted to come up with some less obvious findings and discuss few of the critical flaws found in more detail, that being said, in more general level concerning the given well known vulnerabilities.

5.2.1 Issues with the port scanning

We attempted to port scan the whole subnet using various NMAP switches. But during our testing we witnessed some strange behavior on the ldil.de firewall. More detailed information about this behavior is presented in heading seven under "Remotely triggerable filtering of ports by the firewall". Nevertheless, we got some results in overall, after combining the results achieved from the Nessus scan and partial results of NMAP scans.

5.3 Workstation network (Internal and branch)

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

We detected some critical vulnerabilities in Windows SMB-service and DNS-service of multiple servers. Those vulnerabilities allow remote code execution in the server or allow those servers to be used in a denial of service attack. Also, support to weak algorithms is enabled in SSH-server.

5.4 Management networks (MGMT, warehouse and staff)

As with all the other main findings presented above, also in management networks most of the systems were poorly updated and therefore many security vulnerabilities were found. As this seems to be “de facto”, author will concentrate to most critical findings.

Logging system includes two servers which are located in MGMT-network. Both of these servers had more than one hundred vulnerabilities, which can be seen as critical problem. These servers are part of monitoring and proactively preventing problems relating to most of the components inside multiple network segment presented in this document. Also, PCI DSS demands implementing automated audit trail for all system components and this function is on most parts on responsibility of these servers. As attack surface is notable wide, it should be taken into account that information stored in these server is not safe and could be deleted or modified quite easily.

Another important notice is F-secure Policy Manager, which is responsible of end-point security. All updates and management relating to companywide end-points are centrally managed through this server. FSPM had also wide attack surface and all these functions can for that reason easily compromised.

Outside the scope of PCI DSS, in warehouse network there was critical HR system which should be noted. As this service includes personal data about employees, any information disclosure relating to this system could cause remarkable reputation harm to company. Also, while general data protection regulation is stepping in, also financial sanctions are possible.

6 Recommendations

In general, the first and foremost task or activity that should take place based on the results of this audit would be to upgrade the software components of the given target systems. This is essential as it would cover majority of vulnerabilities found in systematic and logical manner. To accomplish this, software repositories need updating and possibly reconfiguration.

As with any software upgrade, this task should be split and prioritized so that the most impactful systems are patched first. Yet, to do this in safe and mature manner this patching should be done in pre-production or testing environment before touching the production system. This is key in order to avoid causing mayhem on the production that could occure due to broken software packages or incompabilities introduced by version changes.

Some of the found vulnerabilities are more complex and require configuration changes in addition to software upgrade. Example of this kind of vulnerability would be the weak encryption algorithms. To fix these in safe manner it would be ideal to first check that also the surrounding software stack supports the stonger, more modern, encryption methods.

All in all, the key take away from this report is that the software is largely outdated and needs actions to be taken.

Disable old encryption protocols and update encryption software to newest version.

As addition to technical recommendations, passive review revealed notable absence of documentation. To support decision making, and for example investments related, all services and components should be prioritized as part of risk management activities. In this case chosen framework PCI DSS should create base for these activities. Also, most of the scanned networks included devices that were not included in supplied documentation. There was a logical explanation for presence of most of the devices, but to ensure that any illegitimate devices can’t interact with the network, mitigation methods should be implemented and documentation should updated.

7 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.

7.1 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	1.7.03
Owasp ZAP	2.7.0

7.2 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

7.3 Vulnerability Summary

The purpose of this chapter is to gather an executive summary of all the findings so that it's possible to get a fast general understanding of the state of the cyber security in the Ldil network. (The hosts .222, .234, and .237 for Kali and .251 for Nessus in each network segment are not included in the summary.) Each network segment is detailed separately. The unknown or undocumented services are at the end, otherwise all the host are in ascending order by their IP address.

7.3.1 DMZ vulnerability summary

Internally the services in DMZ contain several vulnerabilities. The most secure service, after the firewall, is the Mail server. Others have several critical and high-risk vulnerabilities. There should be limited access to the internal network segments, but even so, for example the compromise of web-server might prevent the customers from accessing the site and thus hinder the money flow from customers. The internal vulnerabilities are summarized in the table 3. The external, or Internet facing services or addresses, are in the table 4. There is nothing alerting in the Internet facing services.

Table 3 DMZ internal vulnerabilities summary

Host	Service	Critical	High	Med	Low	Info
10.10.10.1	Firewall	0	0	0	0	3
10.10.10.4	ns1	16	89	101	7	38
10.10.10.7	Unknown	0	0	0	0	9
10.10.10.8	ns2	16	89	101	7	38
10.10.10.10	extranet	19	90	131	9	60
10.10.10.20	www	22	95	136	12	69
10.10.10.30	Mail	0	0	11	9	54
10.10.10.40	Helpdesk	19	95	124	7	35

Table 4 DMZ and external vulnerabilities summary

Host	Service	Critical	High	Med	Low	Info
60.254.143.2	Carrier PE	0	0	0	0	8
60.254.143.2	Branch FW	0	0	3	0	0
79.99.193.10	Extranet.ldil.de	0	0	0	0	4
79.99.193.20	www.ldil.de	0	0	0	0	4

7.3.2 Internal and Branch vulnerabilities summary

Internal services contain the Domain Controller for Windows workstations, Fileserver, Intranet and MySQL –database. The two latter ones have 19 critical vulnerabilities and almost a hundred high-risk vulnerabilities each. Through the intranet the malicious actor could have access to all the workstations that access the Intranet. Compromising MySQL –server on the other hand may cause irreparable damage to the database. Also, there was again one host, .91, of which we couldn't find from the service catalog. Again, in the Ldil Cyber Security Implementation report mentions about the Apache server being setup and left un-updated. The summary of the vulnerabilities found in the services is in the table 5.

Table 5 Internal services vulnerabilities summary

Host	Service	Critical	High	Med	Low	Info
10.0.100.10	DC	4	0	9	0	41
10.0.100.20	Files	2	0	0	0	20
10.0.100.30	Intra	0	0	12	4	33
10.0.100.50	MySql	0	0	2	2	23
10.0.100.91	CCTV	0	0	1	0	17

7.3.3 Branch store segment vulnerabilities summary

In the branch store network segment the only critical vulnerabilities, three in total, were on the read only copy of the Domain Controller. There were no high-risk vulnerabilities in any service.

There was, however, a host that wasn't catalogued that should be checked, but the best estimate is that it's an instance of Kali. The summary of the number of vulnerabilities in the branch store segment can be found from the table 6.

Table 6 Branch vulnerabilities summary

Host	Service	Critical	High	Med	Low	Info
192.168.10.10	DC	3	0	1	0	30
192.168.10.20	POS	0	0	3	2	31
192.168.10.30	InfoTV	0	0	0	0	4
192.168.10.51	CCTV-Branch1	0	0	2	0	18
192.168.10.52	CCTV-Branch1	0	0	1	0	18

7.3.4 Management networks vulnerabilities summary

Management network is one of the most critical network segments, since it contains the Log servers, F-Secure Policy Manager and apparently a cluster of management workstations which are, however, undocumented. The computers running logging services and the F-Secure Policy manager have again several critical and in the case of FSPM, more than hundred high-risk vulnerabilities.

The suspected management computers were identified by their DNS or netbios – name, which contains the string k#### (# representing a number). Those have been labeled with “unknown/mgm” in the table 7 below. The hosts .106-.108 are most likely similar management computers, even though the before mentioned string wasn’t found.

On top of the management computers, the hosts .20 and .21, containing Linux, are undocumented in the service catalog. The .20 most likely contains the NetIQ Sentinel based on the hostname and that is documented in the Ldil’s Cyber Security Implementation report. The .21 is the interface for delivering data for the Sentinel.

Of the host .103 no information was found. All the information is summarized in the table 7.

Table 7 Management network vulnerabilities summary

Host	Service	Critical	High	Med	Low	Info
10.99.0.1	Firewall	0	1	8	2	29
10.99.0.10	Log1	12	49	52	8	49
10.99.0.11	Log2	11	49	52	8	49
10.99.0.110	FSPM	10	144	32	2	94
10.99.0.120	PRTG	1	0	4	0	23
10.99.0.130	CCTV-Manager	0	0	3	2	27
10.99.0.20	**Sentinel(?)**	1	0	7	3	35
10.99.0.21	**Sentinel**	0	0	7	3	39
10.99.0.100	**unknown/mgm**	0	0	9	2	25
10.99.0.101	**unknown/mgm**	0	0	9	2	26
10.99.0.102	**unknown/mgm**	1	0	10	3	25
10.99.0.103	**unknown**	0	0	0	3	3
10.99.0.104	**unknown/mgm**	0	0	9	2	25
10.99.0.105	**unknown/mgm**	1	0	10	2	25
10.99.0.106	**unknown**	0	0	9	3	22
10.99.0.107	**unknown**	0	0	9	2	22
10.99.0.108	**unknown**	0	0	9	2	22
10.99.0.109	**unknown/mgm**	2	0	11	2	34
10.99.0.111	**unknown/mgm**	1	0	10	2	25

7.3.5 Warehouse network vulnerabilities summary

The warehouse network segment contains the hosts for running services for Human Resources and Front Accounting. The system running the HR services is again extremely vulnerable, with 19 critical and 90 high-risk vulnerabilities. The summary of the vulnerabilities can be found from the table 8.

Table 8 Warehouse vulnerabilities summary

Host	Service	Critical	High	Med	Low	Info
172.20.0.10	HR	19	90	126	9	52
172.20.0.20	Front Accounting	0	0	0	0	13

7.4 Vulnerability Details

Objective of this title is to issue more technical and detailed information about the most important vulnerabilities presented above. In addition to technical explanation and possible mitigation proposal, overview includes severity to support decision making.

Information is divided based on group responsibilities presented in title four. Full technical records regarding all audit activities are attached to this document.

7.4.1 List of DMZ vulnerabilities from external view

BGP port open

Synopsis: BGP control plane possibly vulnerable

Vulnerable Targets:

79.99.192.1. According to the documentation, this is the RGCE ISP.

Vulnerability Explanation: There is a possible configuration error in form of BGP tcp/179 being reachable from our Nessus scanner. Danger in this configuration is that BGP port is a sign of possibly lacking control plane protections on the ISP router. Possible exploitation vectors include things such as sending RST packet from falsified source address and general overloading of the BGP process on the listening party. Net effect of this is that the would-be BGP peering might be prone to denial of service attacks, given that there is no peerings configured, the BGP tcp/179 should not be open to begin with. Hence, as an exception to the previously mentioned lack of recommended fixes we'd like to point out the following: Assuming that the open BGP port is for future use cases we would like to propose the following mitigation methods.

1) Filter inbound packets based on TTL value - this could be done on both ends of the BGP peering
2) Make sure that the uRPF filters are utilized on both the ISP network in general and in the customer peerings

Severity:

Service port closed for extranet service

Synopsis: HTTP(S) service port closed for a likely HTTP(S) server

Vulnerable Targets: 79.99.193.10, extranet.ldil.de, the Extranet service.

Vulnerability Explanation: Although this server likely hosts HTTP(S) services, the top 1000 ports were all displayed as filtered. This was likely due to feature of the PaloAlto firewall that we'll discuss later on this report.

Severity: Medium

Service port closed

Synopsis: HTTP(S) service port closed for a HTTP(S) server

Vulnerable Targets: 79.99.193.20, www.ldil.de

Vulnerability Explanation: All top 1000 service ports were filtered according to the NMAP and Nessus scans. This doesn't sound right, as the store should definitely serve publicly from ports 80 and 443. This, similarly to the previous finding, will be discussed in further detail later on.

Severity: MEDIUM

Remotely triggerable filtering of ports by the firewall

Synopsis: Traffic rejection treshold prone for remote triggering

Vulnerable Targets: 79.99.193.1, PaloAlto firewall

Vulnerability Explanation: Apparently the PaloAlto firewall starts to shun source addresses that it deems as sources of port scanning. This is all good as such but it provides interesting vector for denial of service attacks as follows. An attacker could forge the source address of the connection so that the source IP address could come from one or more of the critical interest groups. At least some form of whitelisting should take place as uRPF filters are not deployed fully in the Internet and even if the first next-hop ISP did utilize uRPF the whole of Internet does not. Whitelisting of source addresses would mitigate the DoS vector in a simple manner, except that the web store should be reachable from everywhere, hence the source address filter is not enough on its own. Whitelisting the tcp/80 and tcp/443 for web store would mitigate this to some extent. Yet, whitelisting would open the door for flooding the firewall state table for the given whitelisted ports. Hence, the recommendation would be to consider using stateless filters in ISP routers for the mandatory tcp/80 and tcp/443 and do the specific filtering in the PaloAlto firewall for other non "access from anywhere" services utilizing whitelisting.

Severity: HIGH

7.4.2 Vulnerability findings found from inside the perimeter firewall

As scans executed from the outside interface were greatly affected by the behaviour of the firewall, more information about ports and services were gathered by scanning from the private network. This, nevertheless, bypasses the security provided by the firewall. On the other hand, as defence should always be multilayered and should not trust solely a single point of protection, the results can be considered as valid from the point of view of a public network, as the scans executed from therein.

Undocumented device with services open

Synopsis: There are undocumented apparel in the network, with open services
Vulnerable Targets: 10.10.10.7 (Unknown host) (Additionally 79.99.193.251 (Kali), 79.99.193.234 (Nessus) as undocumented devices)
Vulnerability Explanation: First interesting finding was 10.10.10.7. What makes this address so compelling is that there was no mention of this address in the documention e.g. excel sheet. This on its own could be a severe anomaly, especially as we failed to login via SSH using the passwords and usernames available. To increase the importance of this finding was the TFTP server running on the host. We tested this by uploading some files. This means that not only was the host not documented, but it also had write access made available via TFTP. This could be exploited in terms of denial of service by filling the disk on the receiving end, obviously depending on the TFTP configuration. Uncomented IP addresses might be an indication of problems implementing change management and other administrative procedures. Two other undocumented addresses were found, namely Kali and Nessus - obviously these where not present in the time when the documentation was written but these could still be seen as worthwhile indicators of documentation lagging behind.
Severity: CRITICAL

SSH port unfiltered

Synopsis: SSH port open from everywhere

Vulnerable Targets: 10.10.10.10 (extranet.ldil.de)

Vulnerability Explanation: Extranet host had SSH open from everywhere from the local iptables firewall. In practice, the input policy was set to ACCEPT, which thus allows SSH connections from anywhere. Likely this host had no in-depth SSH hardening done.

Severity: MEDIUM

Non-hardened services

Synopsis: Services are not hardened for restricting attack surface.

Vulnerable Targets: 10.10.10.20 (www.ldil.de)

Vulnerability Explanation: Magento host had several issues. To name a few: firstly basic authentication without encryption was detected, PHPMyAdmin was visible and directory browsing enabled as reported by Nessus. No authentication details should be never sent as clear text, as this would make it possible to harvest login details with simple data sniffing. PHPMyAdmin is a web frontend to administer SQL databases. This is a very powerful tool and should be absent in production servers or heavily protected by strict access limiting and other methods. The third problem brought out here is the directory browsing. This feature make it possible to for example gain valuable information about the files and directories available in the system. A good example of this could be a backup file which would make an executable file rendered as a text file providing extensive details about the system, or revealing a htaccess file to reveal the password hashes to the attacker.

Severity: CRITICAL

Plaintext authentication supported

Synopsis: Plaintext authentication for SMTP is supported

Vulnerable Targets: 10.10.10.30 (mail.ldil.de)

Vulnerability Explanation: SMTP host had plaintext authentication supported. This is a possible source of leaking user accounts. It is worth mentioning that the weaknesses in configurations mentioned above on Magento, SMTP and extranet hosts represent the type where simple software update does not likely solve the problem itself. Instead, manual configuration changes are required to mitigate the errors in question.

Severity: MEDIUM

Shellshock

Synopsis: Shellshock, also known as Bashdoor, is a security vulnerability found in the Bourne Again shell (Bash).

Vulnerable Targets: 10.10.10.4 (ns1.ldil.de), 10.10.10.8 (ns2.ldil.de), 10.10.10.10 (extranet.ldil.de), 10.10.10.20 (www.ldil.de), 10.10.10.40 (helpdesk.ldil.de)

Vulnerability Explanation: Shellshock, also known as Bashdoor, is a security vulnerability found in the Bourne Again shell (Bash). Shellshock was seen first time in september 2014, yet this vulnerability appears to be present in LDIL environment likely due to software upgrades being unavailable, since Shellshock is relatively trivial to patch simply by upgrading the bash shell to newer, less vulnerable version.

It should be noted that these where found during the scanning from the *inside* of the network.

These vulnerabilities were not detected during the scanning from outside - this could be due to various factors such as:

- The dynamic manner how the PaloAlto firewall responded to port scanning by blocking the source address during scanning
- Possibly due to packet filtering taking place as expected, Nevertheless, Shellshock opens interesting opportunities for exploitation assuming some means to access the aforementioned hosts inside the packet filtering perimeter.

As previously stated, Shellshock is vulnerability in the Bash shell. More in-depth explanation is that Bash unintentionally executes directives when commands are chained to the very end of the function definitions that in turn are stored values within the system environment variables. What makes Shellshock so nasty is that the way it exploits the Bash function export feature to a net effect of providing user access to functionality that is not supposed to be available to the user executing the Bash shell. This happens since each instance of Bash scans the environment variable list for scripts, and assembles these scripts into a statement that defines the script within the new instance and finally executes the command. Bash has no means to verify the origin or validity of these script definitions. This leads to a scenario where attacker can execute commands on the system or abuse other bugs that might exist in Bash.

Given that the mentioned functionality might sound solely locally exploitable vulnerability, unfortunately this is not the case as various pieces of remotely reachable software - such as web servers - might utilize Bash to execute functions such as system(). This means that Shellshock is not only locally exploitable. As a proof of this in the first phases Shellshock announcement it was actively exploited by DoS practitioners, mostly to build botnets utilized in DDoS attacks.

Business impacts of the attack vector: This being said, ldil.de runs largely on top of web servers hosted on Linux environment when bash tends to be the default shell. This sets the ground for urgency of updating the shell since shellsock provides ground for taking out or corrupting part of the core business infrastructure, namely the web shop. This is also key element in terms of fulfilling the PCI DSS security requirements set for the platform producing the service. These are obvious fail-factors for audit.

Severity: CRITICAL

Weak cryptographic ciphers

Synopsis: This is a general discussion concerning the known weak cryptographic ciphers found from ldil.de environment. We will also discuss few of the known vulnerabilities related to weak ciphers, namely arcfour (eg. alleged RC4), CBC and

weak MAC algorithms. These weak ciphers were found from multiple hosts in the ldil.de environment, for instance the Magento based web shop. This on its own is a significant business risk as ldil.de relies largely on the web shop infrastucture to work.

Vulnerable Target: 10.10.10.20 (www.ldil.de), 10.10.10.10 (extranet.ldil.de), 10.10.10.0/24: all host for SSH issues.

Severity: CRITICAL

Vulnerability Explanation: By using weak ciphers it is possible that for example some or all parts of the encrypted message could be made readable by offender. This is especially critical for administrative traffic, since administrative infrastructure can be seen as one step more confidential than the production environment being administrated, namely restricted environment could be administrated from a secret administration environment.

Since it is in practice possible to use only computationally secure algorithms it is a good idea to make sure that the algorithms used are not too quick, cheap or trivial to reverse without immense computing power. Thus, it is greatly discouraged to use bad ciphers which for example RC4 is with its several known flaws.

CBC (Cipher Block Chaining) used in SSH also has known vulnerabilities. By taking advantage of these vulnerabilities, an attacker might recover plaintext from the ciphertext. Thus it is strongly adviced to disable CBC from cipher sets. The last issue discussed here is the use of weak MAC algorithms. MAC (Message Authentication Code) algorithms are used to ensure integrity of the messages. Integrity issues as such don't reveal the secured data directly, but as integrity is still a basic part of security, the weaknesses should not be around on purpose. In this case for example, MD5 is used as one possible algorithm. MD5 is prone to hash collisions with very little effort, thus it is fairly trivial to falsify the message whilst keeping the MD5 sum identical to the original one.

Weak algorithms are especially critical in web shop applications which, when exploited, can have severe complications in terms of loss of reputation, client data and business. Several weak algorithms have for example known man-in-the-middle attack methods, which make it possible to capture the traffic by a malicious third

party. Attacks like POODLE, which was identified by Nessus in several services, could be used to launch an attack of this sort.

In general, it is very important to keep all communication data properly encrypted, by using recommended crypto settings. Usually communication happens on top of a less secure media, for example the Internet, which can not be fully controlled by the administration and data protection plays a huge part in there. It should be noted that while some of the issues mentioned here could have been mitigated by updating the relevant packages - assuming those where available in RGCE to begin with - there is also need for changes in application server configuration in order for the weak ciphers to be disabled. This emphasises the importance of change management and keeping up with latest security bulletins, such as NCSA mailing list.

Business impacts of the attach vector: These ciphers are part of the webshop environment, but their effects can be seen in other services as well, such as SSH. SSH, being used for maintenace tasks makes it even more critical for these vulnerabilities to get patched the soonest. This makes encryption a critical audit criteria.

7.4.3 List of vulnerabilities in workstation networks and WEB services

Vulnerability in DNS Resolution

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

Vulnerable Targets:

files.ldil.de / 10.0.100.20

dc.ldil.de / 10.0.100.10

rodc.ldil.de / 192.168.10.10

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: CRITICAL

Microsoft Windows SMB Server vulnerabilities

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

Vulnerable Targets:

dc.ldil.de / 10.0.100.10

files.ldil.de / 10.0.100.20

rodc.ldil.de / 192.168.10.10

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: CRITICAL

Vulnerability in DNS Resolution Could Allow Remote Code Execution

Synopsis: MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution.

Vulnerable Targets:

dc.ldil.de / 10.0.100.10

rodc.ldil.de / 192.168.10.10

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

Vulnerability in Schannel Could Allow Remote Code Execution

Synopsis: The remote Windows host is affected by a remote code execution vulnerability.

Vulnerable Targets:

dc.ldil.de / 10.0.100.10

Vulnerability Explanation:

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

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

Outdated jQuery library in use

Synopsis: jQuery library is outdated and possibly vulnerable to exploits

Vulnerable Targets: http://intra.ldil.de / 10.0.100.30

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

Outdated PHP version in use

Synopsis: PHP framework is outdated and possibly vulnerable to exploits

Vulnerable Targets: http://intra.ldil.de / 10.0.100.30

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

Verbose information about system version available in http response

Synopsis: HTTP response includes information the operating system.

Vulnerable Targets: http://intra.ldil.de / 10.0.100.30

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

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 / 10.0.100.30

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

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 / 10.0.100.30

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

Proof of Concept Code Here:

GET

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

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 / 10.0.100.30

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

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: http://intra.ldil.de / 10.0.100.30

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

X-frame-options header not set

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

Vulnerable Targets:

http://intra.ldil.de / 10.0.100.30

http://helpdesk.ldil.de / 10.10.10.40

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

SSH Weak Algorithms Supported

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

Vulnerable Targets: pos.ldil.de / 192.168.10.20

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: Update and configure SSH server to disable weak algorithm.

Severity: MEDIUM

HTTP TRACE / TRACK Methods Allowed

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

Vulnerable Targets: http://pos.ldil.de / 192.168.10.20

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

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 / 10.0.100.30

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

8 Attachments

Table 9 Attachment files

Attachment name	Attachment description
01_StoreBranch_Nessus_portscan.pdf	Nessus port scan of store branch network segment
02_Internal_Nessus_portscan.pdf	Nessus port scan of internal network segment
03_MGMT_Windows_Nessus_scan.pdf	Nessus Windows scan of Management network segment.
04_MGMT_Linux_Nessus_scan.pdf	Nessus Linux scan of Management network segment
05_DMZ_Outside_Nessus_scan.pdf	Nessus scan of the Internet facing host(s)
06_ DMZ_Inside_Nessus_scan.pdf	Nessus scan of the DMZ
07_Warehouse_Nessus_scan.pdf	Nessus scan of the Warehouse network segment
08_Staff_Workstations_Nessus_scan.pdf	Nessus scan of the Staff Workstations network segment
09_Branch_Staff_Workstations_Nessus_scan.pdf	Nessus scan of the Branch Staff Workstations