jamk.fi

Final Raport

Author Adam Pawełek

Teacher: Markku Vajaranta
Autor of Assignment: Adam Pawełek
Group: TTKS0700-3001
Jamk number: AA4917
Email: aa4917@student.jamk.fi

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

1 Table of Contents

1 Question 1 3

2 Question 2 5

2.1 Subsection A 5

2.2 Subsection B 7

3 Question 3 8

3.1 Find out lack in Security: 8

3.2 Some variabilities connected to previous points. 9

3.3 OpenSSH 5.9p1: 9

3.4 Appache 2.2.22 (Vulnerabilities with score 7.5 CVE Details) 11

3.5 Linux Kernel 3 (Vulnerabilities 10) 12

3.6 Debian 5 (Vulnerabilities above score 9) 15

4 Question 4 17

4.1 Threats aggents: 17

4.2 Possible atacks: 17

4.3 Estimate likelihood of attacks 19

4.4 Estimate the impact of attacks 19

5 Question 5 21

5.1 What is fuzz testing? 21

5.2 Name two items from OWASP top 10 web vulnerabilities list and explain them 21

5.2.1 Injection: 21

5.2.2 Using Components with Known Vulnerabilities: 21

5.3 What is an attack vector? 22

5.4 What does “Anomaly” mean and how is it related to cybersecurity? 22

5.5 What is CVSS and how is it related to vulnerabilities? 23

5.6 What does the Finnish legislation say about using a network/vulnerability scanners like nmap/openvas? 23

1 Question 1

CEO of the Cool Architectures has planned to start auditing their infrastructure. Describe the auditing process. Use max 2 pages.

First I would like to write about 3 basic types of audit and about the differences between them.

Internal Audit
1.First Party Audit -> The audit is carried by auditee. (This is basic audit. Problem with this kind of audit is that you are auditing your own work and you could overlook some disadvantages of your system/ work).

External Audit:

2. Second-party audit -> The audit is carried by the person which have the same interest as auditee (for example If you want to do audit for your sub-contractors or your costumers do audit in your company)

3.Third-party audit -> The person/company doing the audit is totally independent from your business. Those are external companies which are only checking if you to fulfil the criteria.

CEO of our company should also choose standardization level (International, Regional, National) which will be based audit on. Before external audit our company could do internal audit and use also Checchi's like Katakri.

Based on this information I could start describe auditing process.

Audit process:

Planning

1. Audit subject (In our case it will be security of network and servers and knowledge workers about network safety)
2. Audit object (Network, Servers, Firewall)
3. Audit Scope (In this audit we should check safety of our network, servers, firewall. We could also check the technical aspects of our equipment. If this equipment is safe enough (For example, do the cables used for communication prevent eavesdropping?). We should also check if ours workers could recognize phishing attacks.
4. Procedures (Company safety procedures this is required to find out if company is secured against human error for example phishing attacks)
5. Assets which company have and wants to protect them

Testing and Documentation:

1. Preliminary research (This part is for recognize which part of our network could be weak and vulnerable to attacks)
2. Test Controls (This part test our network which different standardization test and list)
3. Discovery and validation (This step is to prove that all procedures, process, and equipment works properly and show all lack in security).
4. Collect rules (Collect all rules which works properly and lack in others rules)
5. Document Results

Analyses and reporting

1. Risk Analyses based of previous documented results

2. Recommendation for increasing security

3.Technical Report (Final report showing the strengths and weaknesses of our networks.)

4.Menagement results (Checking whether our network meets the previously defined standards.)

Source of steps -> Presentaion 02A. Audit basics.

2 Question 2

2.1 Subsection A

As the auditing carries on, you did vulnerability scanning from the Internet to the company firewall. Results showed the Wordpress to have two vulnerabilities: CVE-2014-0160 and CVE-2016- 5837. What are these vulnerabilities and which of them is more important to be fixed? Why? (If you used some public source for this, please add it (syntax and method how you add the references is very free-form).

CVE-2014-0160 Detail

Current Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Evaluator Impact

CVSS V2 scoring evaluates the impact of the vulnerability on the host where the vulnerability is located. When evaluating the impact of this vulnerability to your organization, take into account the nature of the data that is being protected and act according to your organization's risk acceptance. While CVE-2014-0160 does not allow unrestricted access to memory on the targeted host, a successful exploit does leak information from memory locations which have the potential to contain particularly

sensitive information, e.g., cryptographic keys and passwords. Theft of this information could enable other attacks on the information system, the impact of which would depend on the sensitivity of the data and functions of that system.

Source -> https://nvd.nist.gov/vuln/detail/CVE-2014-0160

CVE-2016-5837 Detail
Current Description

WordPress before 4.5.3 allows remote attackers to bypass intended access restrictions and remove a category attribute from a post via unspecified vectors.

Source -> https://nvd.nist.gov/vuln/detail/CVE-2016-5837

A remote user can remove a category from a post [CVE-2016-5837]
Source -> https://securitytracker.com/id/1036163

What are these vulnerabilities and which of them is more important to be fixed? Why?

We should fix first CVE-2014-0160 vulnerability because this lack in security may lead to obtain sensitive information. CVE-2016- 5837 vulnerability allows attacker only to remove category from WordPress post. Remove category from WordPress post may lower number of website views because google algorithm could not find key words in search. Obtains sensitive information could conduce to large fines and lost of trust with our clients that's why we should first fix CVE-2014-0160 vulnerability.

2.2 Subsection B

All workstation machines in the Cool Architectures are running Windows 10, and the domain controller and file servers Windows server 2019. Internal scanning did not reveal any high nor medium level problems in the network. What recommendations would you still have regarding the company infrastructure?

-There is no DMZ (demilitarized zone). This network should have DMZ it will increase network security.

-Network should not allow all ports from VLAN 44 to VLAN 88 and from VLAN 88 to VLAN 44.

-Only some workstation need access to fileservers. If some workers don't need access to fileservers we shouldn't allow access them. If workers won't be correctly trained in security may be potential source of risk (phishing attacks)

-This network should also have IDS or IPS systems.

-This network might have better firewall for example Palo alto router firewall because as we seen in attachment 3. Nmap get to easy all information about company network.

-This network should also have some tools, devices which will search for attackers and alert Security operations center company about potential threats like Fidelis Endpoint. Source - > https://fidelissecurity.com/products/endpoint

-This network should have some tools which will confuse attackers imitate valuable data and servers and mislead the attacker to wrong paths. (For example Fidelis Decetpion) Source -> https://fidelissecurity.com/products/deception

-Company network don't have any backup servers. It should have backup servers in another WLAN network.

3 Question 3

A new web server is being installed to the Cool Architectures by a summer job employee and you have been assigned to do a quick scan with an nmap to this new web server in your company. What can you find out, especially in security wise, from the results that are illustrated in the Attachment 3?

3.1 Find out lack in Security:

http-methods should have disabled OPTIONS unless is really necessary for debugging or some Rest Api. This is not variability but could give attacker some valuable information.

http-server-header: Apache/2.2.22 (Ubuntu) -> Name of the webserver is not hide (even version of Apache) this may help attackers find variabilities and attack easier company site.

Upgrade OpenSsh current version OpenSSH 5.9p1 newest version : OpenSSH 8.4

Upgrade kernel: linux_kernel:3, newest stable Linux kernel : 5.9.11

Upgrade Debian: Current version Debian 5 (2012-02-06 : End of security updates / End of life). The latest stable release of Debian is 10.6.

-Change firewall for better this firewall should notice nmap scanning (this scanning was with T4 speed. This scan was not even pretending normal traffic)

-Webserver (Apache) is working on port (80) http no on port 443 (https) it will be more secure to run it at port 443.

-Update Apache newest version is (2.4.46) verion on server (2.2.22)

3.2 Some variabilities connected to previous points.

(Descriptions are copy from site CVE Details to facilitate reading variabilities).

3.3 OpenSSH 5.9p1:

- CVE-2018-15919

Description:
Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

Source -> https://www.cvedetails.com/cve/CVE-2018-15919/

- CVE-2017-15906

Description:

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in read-only mode, which allows attackers to create zero-length files.

Source -> https://www.cvedetails.com/cve/CVE-2017-15906/

- CVE-2016-10708

Description:

sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.

Source -> https://www.cvedetails.com/cve/CVE-2016-10708/

- CVE-2016-0778

Description:

The (1) roaming read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.

Source -> https://www.cvedetails.com/cve/CVE-2016-0778/

- CVE-2016-0777

Description:

The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by

reading a private key.

Source -> https://www.cvedetails.com/cve/CVE-2016-0777/

3.4 Appache 2.2.22 (Vulnerabilities with score 7.5 CVE Details)

-CVE-2013-2249

Description:

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

Source - > https://www.cvedetails.com/cve/CVE-2013-2249/

- CVE-2017-3167

Description:

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

Source -> https://www.cvedetails.com/cve/CVE-2017-3167/

- CVE-2017-3169

Description:

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

Source -> https://www.cvedetails.com/cve/CVE-2017-3169/

- CVE-2017-7668

Description:

The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.

Source -> https://www.cvedetails.com/cve/CVE-2017-7668/

- CVE-2017-7679

- In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Source -> https://www.cvedetails.com/cve/CVE-2017-7679/

3.5 Linux Kernel 3 (Vulnerabilities 10)

-CVE-2014-2523

Description:

net/netfilter/nf_conntrack_proto_dccp.c in the Linux kernel through 3.13.6 uses a DCCP header pointer incorrectly, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a DCCP packet that triggers a call to the (1) dccp_new, (2) dccp_packet, or (3) dccp_error function.

Source -> https://www.cvedetails.com/cve/CVE-2014-2523/

- CVE-2015-0573

Description:

drivers/media/platform/msm/broadcast/tsc.c in the TSC driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (invalid pointer dereference) or possibly have unspecified other impact via a crafted application that makes a TSC_GET_CARD_STATUS ioctl call.
Source -> https://www.cvedetails.com/cve/CVE-2015-0573/

-CVE-2016-2063
Stack-based buffer overflow in the supply_lm_input_write function in drivers/thermal/supply_lm_core.c in the MSM Thermal driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted application that sends a large amount of data through the debugfs interface.
Source -> https://www.cvedetails.com/cve/CVE-2016-2063/

- CVE-2016-2065
Description:
sound/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (out-of-bounds write and memory corruption) or possibly have unspecified other impact via a crafted application that makes an ioctl call triggering incorrect use of a parameters pointer.

Source -> https://www.cvedetails.com/cve/CVE-2016-2065/

-CVE-2016-5344
Description:

Multiple integer overflows in the MDSS driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service or possibly have unspecified other impact via a large size value, related to mdss_compat_utils.c, mdss_fb.c, and mdss_rotator.c.

Source -> https://www.cvedetails.com/cve/CVE-2016-5344/

-CVE-2018-20961

Description:

In the Linux kernel before 4.16.4, a double free vulnerability in the f_midi_set_alt function of drivers/usb/gadget/function/f_midi.c in the f_midi driver may allow attackers to cause a denial of service or possibly have unspecified other impact.

Source -> https://www.cvedetails.com/cve/CVE-2018-20961/

-CVE-2019-11811

Description:

An issue was discovered in the Linux kernel before 5.0.4. There is a use-after-free upon attempted read access to /proc/ioports after the ipmi_si module is removed, related to drivers/char/ipmi/ipmi_si_intf.c, drivers/char/ipmi/ipmi_si_mem_io.c, and drivers/char/ipmi/ipmi_si_port_io.c.

Source -> https://www.cvedetails.com/cve/CVE-2019-11811/

-CVE-2019-15292

Description:

An issue was discovered in the Linux kernel before 5.0.9. There is a use-after-free in atalk_proc_exit, related to net/appletalk/atalk_proc.c, net/appletalk/ddp.c, and net/appletalk/sysctl_net_atalk.c.

Source -> https://www.cvedetails.com/cve/CVE-2019-15292/

3.6 Debian 5 (Vulnerabilities above score 9)

- CVE-2008-5500

Description:

The layout engine in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to cause a denial of service (crash) and possibly trigger memory corruption via vectors related to (1) a reachable assertion or (2) an integer overflow.

Source -> https://www.cvedetails.com/cve/CVE-2008-5500/

-CVE-2009-4538

Description:

drivers/net/e1000e/netdev.c in the e1000e driver in the Linux kernel 2.6.32.3 and earlier does not properly check the size of an Ethernet frame that exceeds the MTU, which allows remote attackers to have an unspecified impact via crafted packets, a related issue to CVE-2009-4537.

Source -> https://www.cvedetails.com/cve/CVE-2009-4538/

-CVE-2010-0159

Description:

The browser engine in Mozilla Firefox 3.0.x before 3.0.18 and 3.5.x before 3.5.8, Thunderbird before 3.0.2, and SeaMonkey before 2.0.3 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the nsBlockFrame::StealFrame function in layout/generic/nsBlockFrame.cpp, and unspecified other vectors.

Source-> https://www.cvedetails.com/cve/CVE-2010-0159/

-CVE-2008-0017

Description:

The http-index-format MIME type parser (nsDirIndexParser) in Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 does not check for an allocation failure, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an HTTP index response with a crafted 200 header, which triggers memory corruption and a buffer overflow.

Source-> https://www.cvedetails.com/cve/CVE-2008-0017/

4 Question 4

Make following risk assessment steps: identify threat agents and possible attacks, estimate likelihood of attacks and estimate the impact of attacks for the Cool Architectures. The CEO said that he's not sure, but for his best knowledge company assets are the architecture plans located in the file servers.

4.1 Threats aggents:

-hackers
-workers which wants to stole the data
-guest of comapny which can acces the VLAN 44 and stole data from VLAN 88.
-Security experts from others competitive companies.
We could add here also employee which are not trainee in security procedures. They may infect workstations in VLAN 44 with malicious software without their knowladge.

4.2 Possible atacks:

-Phishing attack
-social engineering attack
- Business Email Compromise

-Zero-day exploit
-Drive-by Attack
-Cross-site scripting (XSS) attacks
-Password Attack (if comapny didn't have any special password procedures attacks

like Brute-Force or Dictionary Attacks could work)
-Injection attack

Attacks involve human errors:

The easiest way to carry out attack is to involve workers of company to infect in some way their computer they could open malicious sites which could install malicious software, Attackers may also send attachment which contains viruses or even attackers could pretend to be someone else for example (security designer) and get some sensitive information's. Last but not least the workers could also connect the USB flash drive which could content viruses.

A lot of data in our network and server (which was start by summer employee is not protected) for example kernel version, which apache version webserver use). Also in this server is installed outdated software which have a lot of well-known vulnerabilities.

Using Components with Known Vulnerabilities
Server which was starts by summer employee is exposed to attacks which allow attackers to infect server, steal the sensitive date and crash the server.

This network don't have any DMZ (demilitarized zone). If someone will attack webserver / WordPress server and get access to VLAN 88 network that person will easy steal data from fileservers.

Employee have no limited access from VLAN 44 to VLAN 88. It means that if some computer will be infected in VLAN 44 it could have access to sensitive information's in fileservers and could broke the WordPress server.

WordPress server have 2 vulnerabilities which one is very important to fix. CVE-2014-0160 vulnerability can result leak of sensitive information's from which company could bear the financial costs. It may also help attacker with the next attack. Second vulnerability may lower website income by removing category from WordPress post.

It could be also good idea to separate fileservers which contains most important information's (like company assets) from servers which contains normal information's.

This network doesn't have endpoints, systems which will confuse attackers, have weak firewall (scan nmap with T4 speed). Very good hacker should not have many problems with accessing VLAN 88.

4.3 Estimate likelihood of attacks

Likelihood of attack is average because this company is small and not very well known (this company doesn't have to manage with threads like Samsung, Microsoft). This company could also be attacked with accidental installed viruses by workers which can have big consequences. If Cool Architectures company will increase their security their likelihood of attacks could decrease to low.

4.4 Estimate the impact of attacks

Impacts of attacks could be very serious. If someone access to VLAN 88 will be able to stole company assets which are the architecture plans located in the file servers. That person could also delate this files which could means lost of months of work. Attacker which will have access VLAN 88 could also broke WordPress server and delate

files in it. This will result that WordPress website will no work some time and website will have to be recover from backup if backup exist. If not the website will have to be designed one more. Moreover from VLAN 88 you could access to VLAN 44 and infect all workstations in which malicious software could delate important files or broke windows which may consequence in install Windows from backup or install Windows from the beginning.

If attacker will access to VLAN 44 impacts of attacks will be exactly the same because from VLAN 44 all traffic is allowed to VLAN 88.

5 Question 5

5.1 What is fuzz testing?

Fuzz testing is a technic which tests the reliability of the software application. This technic inject random unexpected input values to find out if application have any crashes, memory leak or failing built-in code assertions.

5.2 Name two items from OWASP top 10 web vulnerabilities list and explain them

5.2.1 Injection:

Injection such as SQL,NOSQL,OS or LDAP injection. Unsecured input for example for login and password can be used for send malicious data with script. For example after inject malicious SQL code it can return queries with sensitive data or delate data in our database.

5.2.2 Using Components with Known Vulnerabilities:

Using components such as libraries, frameworks, APIs and other software modules with well know variabilities could be easy target for attacker. Exposed Vulnerable component may result to data loss or infected server

5.3 What is an attack vector?

Attack Vector is a path/way which attacker gain unauthorized acces to network/computer. This path may exploit for exampe system vulnerability or human naivety.

Source:

-> https://securitytrails.com/blog/attack-vector

->https://www.upguard.com/blog/attack-vector

->https://www.sumologic.com/glossary/attack-vector/

5.4 What does “Anomaly” mean and how is it related to cybersecurity?

Definition -> something that is unusual enough to be noticeable or seem strange

Source -> https://dictionary.cambridge.org/dictionary/english/anomaly

(Cambridge Dictionary -> Us Dictionary)

In cybersecurity anomalys are related for example in NBAD (Network behavior anomaly detection). NBAD for example is searching for anomalies in Network. Check them and if it will discover threats in the network it will block or delate them.

5.5 What is CVSS and how is it related to vulnerabilities?

CVSS -> Common Vulnerability Scoring System is a free and open industry standard that gives you a numerical representation (0-10) of the severity of an information security vulnerability. CVSS scores are calculated based on formula which depends of factors like impact of exploit and how easy is to exploit this vulnerability. Relation between CVSS and specific vulnerability tell us how important it is to fix this vulnerability and when we have list of vulnerabilities suggest us which we should fix first.

5.6 What does the Finnish legislation say about using a network/vulnerability scanners like nmap/openvas?

In Finland is forbiden to scan someones network, organization network, public network. You could use this tools only in your LAN network for security perpuses.

Example of penalties for port scaning.
A 17-year-old Finn was accused of attempted computer break-in by a major Finnish bank. On April 9, 2003, he was convicted of the charge by the Supreme Court of Finland and ordered to pay US$12,000 for the expense of the forensic analysis made by the bank. In 1998, he had port scanned the bank network in an attempt to access the closed network, but failed to do so.