jamk.fi

Final report

Data security testing

Jere Pesonen, M3227@student.jamk.fi

Marraskuu-20
Tieto- ja viestintätekniikka
Tekniikan ja Liikenteen ala

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

1 Network auditing process

In auditing, the network infrastructure (software and hardware) is measured against a standard.

First part of audit is planning. Auditor must come up with audits subject and scope like, what to audit and what to not. When auditing a company's network, the auditor should be aware of everything the network consists of. Every machine, operation systems, patch notes, software's and such are essentially important. Nextly, auditor does some research based on the environment, and sorts out all threads or anomalies, that might come out throughout the audit. He also plans all the procedures that are about to be used throughout the process.

Second thing is doing perform the audit and planned tests, and document it properly. Auditor performs the tests planned before, analyzing the outcome and deviations, and collect the results for further analysis.

Last thing is to analyze the results and doing a proper report to the audited infrastructures holders. Analyzing consists of going through the assets and deviations that popped up in the audit and evaluating the risks that they might provide. Auditor compiles recommendations for network administrators, of how to improve the infrastructures safety based on the audit reports.

2.

CVE-2014-0160 is bug in the OpenSSL 1.0.1 - 1.0.1f where TLS and DTLS implementations can't properly handle Heartbeat extension. This leads to that attacker cam read the memory of the systems protected by the OpenSSL.
https://heartbleed.com/

CVE-2016-5837 is a bug in WordPress, where hacker could modify the site to make it unsafe. Like cross-site scripting, bypassing restrictions, obtaining sensitive revision-history information, and mounting a denial of service.
https://www.debian.org/security/2016/dsa-3639

These vulnerabilities seem fairly equal, since they both can be used to malicious acts. Also, their cvss scores are actually identical. IMO the "CVE-2016-5837" vuln would be more mandatory to fix because it can cause more hazardous possibilities for hackers (like xss and all mentioned before). OpenSSL bug just causes data leaks (which may also be bad.).

3.

Firstly, I notice that https port is closed. It should be up and running, and all traffic to the website should use https. Web server is running Apache httpd 2.2.22, which is outdated and vulnerable. Same thing with OpenSSH version 5.9p1, which for example is vulnerable to Mitm attack. System OS Linux 3.2.8 also has vulnerabilities and should be updated to newer version.

4.

Probable goals for threat agents might be news coverage. Especially smaller and lately started cyber-criminal organizations. might be to get known in the field, spread their name, and gain fame and publicity.

Also, financial gain is something hackers and hacker are seeking. Financial benefit could consist of extortion or acquiring sensitive information that can interest potential buyers.

Cool architectures might end up to target, if attackers are executing automate attack, where they can attack multiple small businesses simultaneously.

I would estimate that likelihood of a hacker attack against small Finnish architecture business is quite small, but it's likely it is going to happen every once in a while. Phishing mails are received almost daily. The larger attack against system would be likely maybe once in a year or two.

Impact of the attack could be moderate **(**significant damage). Even the company is small, it still may have the most to lose. It might have major consequences if it gets hacked.

5.

A. Fuzz testing is a software testing technique, to teste the robustness of the software. Fuzzing uses invalid, unexpected, and random inputs to reveal if there is any bugs or memory leaks in the system.

B. **Injection** risks appear as flaws in databases operation systems or protocols, which accepts untrusted input to program. (command or query).

Sensitive data exposure. The sensitive data in web applications or APIs is not protected properly. This occurs a possibility for attackers to modify or steal the data.

C. **Attack vector** is a type of vector created to approach the security testing of a complex scope in an organized manner.

D. Anomaly is an unidentifiable element or act that hasn't been controlled and can't be accounted for a normal operation.

E. CVSS is Common vulnerability Scoring System is procedure that creates rating based to the seriousness of the vulnerability. It provides a value that can be used for estimating the risk. The bigger the value, higher the seriousness of vuln.

F. Scanning networks and software's, you don't have permitted access to, is illegal. I would assort it to data breach, or minor data breach, which scanner can be guilty of. Legitimation says, that: "Found guilty of Data breaching can occur, if one is gaining information/data from the system that he has no permission to access."