



HELSINKI UNIVERSITY OF TECHNOLOGY



A study of Network Perimeter Security

A Software Business Lab Report, © May 2010

Summary

In January 2010 a network security study was conducted as part of ongoing research by the Software Business Research Unit (SBL) at the Helsinki University of Technology (now Aalto University)¹. The study was conducted to identify the most common security vulnerabilities in an effort to help companies improve their IT security and vulnerability management effort.

During the study the researchers analyzed computer systems of Finnish organizations for software security vulnerabilities that are exposed to the public internet. All participating organizations had given their consent for the conducted vulnerability scans and were afterwards informed about the indentified weaknesses in their systems. The vulnerability analysis revealed a total of 523 weaknesses on 42 hosts run by 32 different organizations.

The study used the vulnerability scanning solution OUTSCAN, provided by Outpost24² and received support from the Finnish Funding Agency for Technology and Innovation (TEKES)³ through the VALO project.

¹ <http://www.bit.tkk.fi/>

² <http://outpost24.com/>

³ <http://www.tekes.fi/en/>

Intro

This study analyzed vulnerabilities in networked computer systems that are accessible from the internet. Vulnerabilities are defects, bugs or misconfigurations in software that can be exploited by an attacker to compromise the confidentiality, integrity or availability of information. Vulnerabilities in networked systems are a major source of today's information security risks, as they expose an organization and its assets to external threats like black-hat hackers, crackers or plain criminals. New vulnerabilities are discovered every day and by the time of this writing⁴, the U.S. National Vulnerability Database⁵ (NVD) holds well over 41,000 known vulnerabilities. Thus, organizations that rely on dependable information systems need to frequently assess their exposure to these vulnerabilities in order to be able to manage their risk. Today, vulnerability management is no longer just a technical need, it has become a legal requirement for many organizations that seek to fulfill modern compliance regulations and conduct business internationally.

We present the results of a recent vulnerability exposure assessment conducted in 32 different organizations. The results show the most vulnerable system types, service families and network ports. They further evaluated differences in the risk exposure of organizations with different kinds of vulnerability management practices such as regular automated vulnerability scans.

Key findings:

- High-risk vulnerabilities make up on third (33%) of the total number of identified vulnerabilities.
- A large part of the analyzed organizations (47%) suffered from such high-risk⁶ vulnerabilities. However, 41% managed to have neither high nor medium-risk vulnerabilities.
- Organizations that manage their vulnerability exposure through regular vulnerability scans or security audits show a tendency of reduced risk exposure compared to other organizations.
- The most common vulnerability had an average CVSS severity score⁷ of 5.86 (at a standard deviation of 1.79) and is found on a web server running PHP behind the ports 80 or 443.

⁴ March 2010

⁵ <http://nvd.nist.gov/>

⁶ Vulnerabilities with a CVSS score of 7 or more are considered „high-risk“. Below 7 is medium, below 4 is low.

⁷ The Common Vulnerability Scoring System (CVSS) measures the relative severity of a vulnerability on a scale from 0 (low) to 10 (high). CVSS is used by the National Vulnerability Database (NVD). Specification available online at <http://www.first.org/cvss/>

Analysis

The following analysis is based on the assessment of 523 Vulnerabilities on 42 hosts in 32 companies and organizations. To protect the identity of the participating organizations and because the same standard software products like Apache web servers or PHP are used in all organizations regardless of their size, headcount or business area we have excluded that information from the assessment. The purpose of the analysis is not to provide statistical proof for particular claims, but to learn from examples to help better protect all organizations' assets.

The results are presented in two parts, Technical and Organization. The first describes details of the identified vulnerabilities while the latter connects them with the vulnerability management perspective.

Technical

Risk factors of vulnerabilities by host type⁸

The identified vulnerabilities were unevenly distributed among the analyzed host types. The largest share of high-risk vulnerabilities was found on web servers, followed by application and security servers. An explanation for the surprisingly high number of vulnerabilities on security servers, such for example firewalls, could be the fact that many of these security systems are themselves based on vulnerable platforms like Linux, Unix or provide user interfaces using insecure PHP/HTTP components.

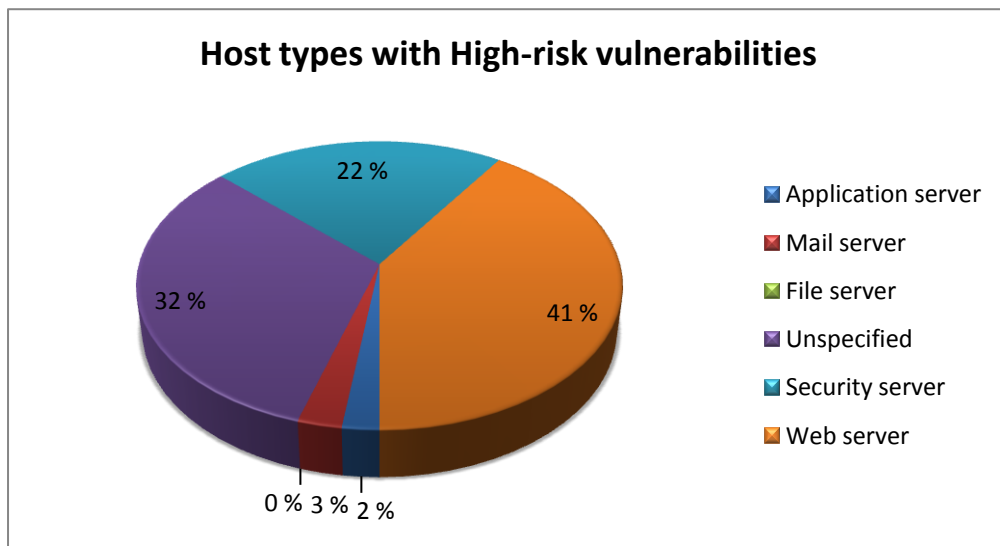


Figure 1 - The share of hosts that suffered from high-risk vulnerabilities - by host type.

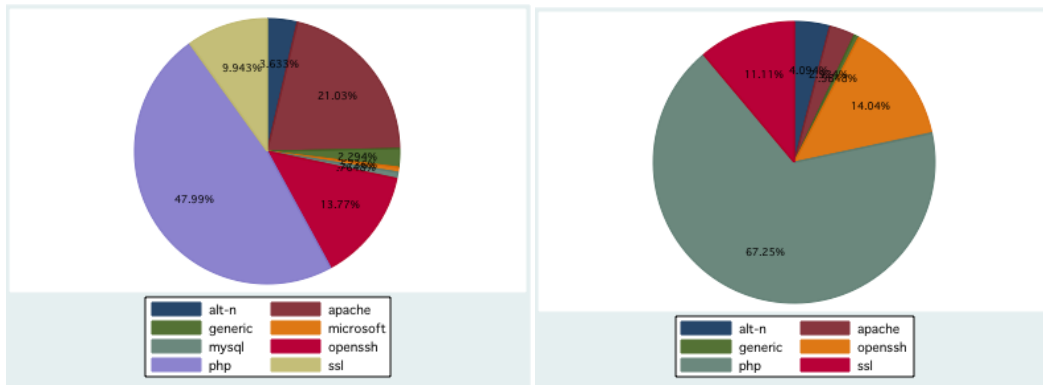
⁸ The type of a server was determined by the it's main use in the organization and not by its technical characteristics such as installed software. The main use was provided by the organization in a pre-study questionnaire.

Table 1 The share of host types that suffered from high-, medium- or low risk vulnerabilities

Host Type	Suffered from vulnerabilities with a risk factor of:			
	High	Medium	Low	Total
Application server	2%	1%	0%	1%
Mail server	3%	1%	0%	1%
File server	0%	0%	0%	0%
Unspecified	32%	80%	74%	71%
Security server	22%	8%	12%	10%
Web server	41%	10%	14%	16%
Total	100%	100%	100%	100%

Vulnerability families

PHP vulnerabilities were overall the most common, followed by those related to the Apache web server and SSH, SSL. When only severe vulnerabilities (with a CVSS score >7) are taken into consideration however, the Apache vulnerabilities are almost insignificant whereas PHP weaknesses dominate the picture.



Left: all vulnerabilities – Right: Vulnerabilities with CVSS score > 7

Most vulnerable ports by share of found vulnerabilities with high-, medium-, or low-risk.

The common web ports 80 (HTTP) and 443 (HTTPS) lead in all risk categories. Most vulnerabilities that were found on the standard SSL port 22 were only of low risks.

Port	Suffered from vulnerabilities with a risk factor of:			
	High	Medium	Low	Total
21	0%	2%	0%	1%
22	9%	8%	26%	10%
25	0%	1%	0%	0%
80	58%	38%	34%	44%
110	4%	4%	5%	4%
443	19%	21%	8%	20%
445	1%	1%	3%	1%
465	1%	0%	0%	0%
587	0%	0%	0%	0%
666	1%	6%	3%	4%
822	5%	3%	11%	4%
995	1%	1%	0%	1%
3306	0%	1%	5%	1%
3389	0%	0%	0%	0%
4242	1%	6%	3%	4%
7600	1%	6%	3%	4%
8088	1%	1%	0%	1%
19638	1%	1%	0%	1%
Total	100%	100%	100%	100%

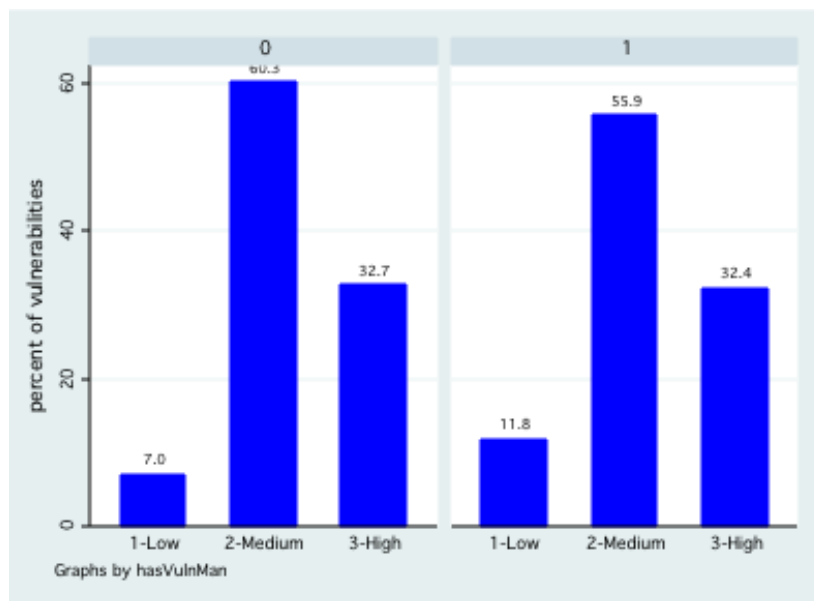
Vulnerability Age

The vulnerability scans were conducted in December 2009 and January 2010. Yet more than half of all identified vulnerabilities had been publicly known since early 2008⁹.

Organizations

Risk Level of Organizations with and without vulnerability management measures.

A quarter (25%) of the analyzed organizations were evaluating their vulnerability exposure on a regular basis either through security audits (9%), automated (16%) or manual vulnerability scans (19%). Organizations that did not conduct such evaluations showed a tendency towards larger numbers of high- and medium risk vulnerabilities on their hosts.



Left: Organizations without vulnerability management activities. Right: Organizations conducting Security audits or automated or manual vulnerability scans.

Average vulnerability severity in organizations

A large part of the analyzed organizations (47%) suffered from high-risk vulnerabilities. However, 41% managed to have neither high nor medium-risk vulnerabilities. The average severity score across all identified vulnerabilities was 5.86 (with a standard deviation of 1.79).

⁹ Age in relation to creation date of their CVE (Common Vulnerabilities and Exposures <http://cve.mitre.org/>) entry. CVE entries may be updated at a later point.

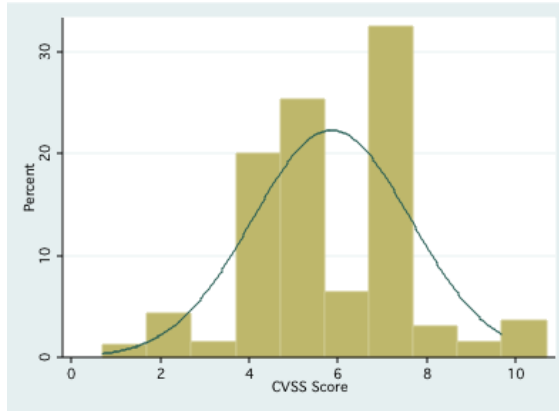


Figure 2 -Histogram of the CVSS scores of all identified vulnerabilities

Table 2 – Organizations that suffered from 1 or more vulnerabilities with a high-, medium-, or low risk factor

Organization	Suffered from 1 or more vulnerabilities with a risk factor of		
	High	Medium	Low
ID001	yes	yes	no
ID002	no	yes	no
ID003	yes	yes	yes
ID004	no	no	no
ID005	no	no	no
ID006	yes	yes	yes
ID007	no	no	no
ID008	no	no	no
ID009	yes	yes	yes
ID010	no	no	no
ID011	yes	yes	yes
ID012	no	no	yes
ID013	yes	yes	yes
ID014	no	yes	no
ID015	yes	yes	yes
ID016	no	yes	no
ID017	yes	yes	no
ID018	yes	yes	no
ID019	yes	yes	no
ID020	no	no	no
ID021	yes	yes	no
ID022	no	no	no
ID023	no	no	no
ID024	no	no	no
ID025	no	no	no
ID026	no	yes	no
ID027	yes	yes	no
ID028	yes	yes	no
ID029	yes	yes	no
ID030	no	no	no
ID031	yes	yes	yes
ID032	no	no	no

Recommendations

Among the participating organizations in this study, many showed a low level of vulnerability exposure and demonstrated that high-risk vulnerabilities are not inevitable. Based on their success, we suggest the following actions to be taken by organization managers and network administrators.

Network administrators

- There are clear hot spots for vulnerabilities: Services related to web servers are among the most common sources for vulnerabilities. These systems are worthy extra attention and should be evaluated more regularly by administrators and their security staff.
- All of the vulnerabilities identified in this study were found using automated vulnerability scanning tools that are publicly available. Administrators should make increasing use of the automated tools in order to be able to reduce their workload and conduct evaluations more frequently.

Organization Managers

- Many of the found vulnerabilities had been publicly known for a long time. Establish an organizational process to find and react on new vulnerabilities in a timely manner.
- As organizations change so do their IT systems and their exposure to vulnerabilities. The more dynamic a network or a system becomes, the more frequent vulnerability exposure assessments should be carried out.