VANJA KORAĆ
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,
E-mail: vanja@mi.sanu.ac.rs

ZORAN DAVIDOVAC
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,
E-mail: zorandavidovac@mi.sanu.ac.rs

DRAGAN PRLJA
Institute for Comparative Law,
Terazije 41, Belgrade, Serbia,
E-mail: dprlja@yahoo.com

004.451.9.056.57
COBISS.SR-ID 254104588

Original research article
Received: March 07th 2017
Accepted: October 31st 2017

LINUX SERVICES VULNERABILITIES ASSESSMENT

ABSTRACT

Tools for analysing vulnerable services on the system can provide valuable information about the status of operating systems in terms of protection. The research in this paper included 29 Linux operating systems. The collected information consists of a large amount of data about the presence of various network services on a system that present potential security flaws. Thus, the vulnerabilities of Linux operating systems that are installed by default (with certain added services) are presented, with the aim of pointing out potential security vulnerabilities. These vulnerabilities or omissions can occur due to incorrectly configured services, well known bugs in the system or program, an outdated system and its services, and the use of poor protection in configuration. The purpose of this assessment is to identify security flaws (vulnerable services) on Linux systems installed by default.

KEYWORDS: VULNERABILITY ANALYSIS, VULNERABILITY ASSESSMENT, LINUX VULNERABILITIES, OS VULNERABILITIES.

By using tools for analysing vulnerable services on the system it is possible to obtain valuable information about the system and the network in terms of protection.[1] As will be shown, the collected information will include a large number of data on the presence of various network services on the system that present potential security flaws. These omissions can occur due to incorrectly configured services, well known bugs in the system or program, an outdated system and its services, as well as the use of poor protection in configuration. The task of this test is to identify vulnerabilities in order to correct all recognized security flaws (vulnerable services) on the systems that are installed by default. All relevant sources reporting vulnerabilities on systems are included and shown in Table 1.

The vulnerability problem can also be seen through the Symantec Vulnerabilities Report for

1 The article results from the project: *Viminacium, Roman city and military camp – research of the material and no material culture of inhabitants by using the modern technologies of remote detection, geophysics, GIS, digitalization and 3D visualization* (no 47018), funded by The Ministry of Education, Science and Technological Development of the Republic of Serbia.

Source name	Web address of the source
APPLE-SA (Apple Security Announce)	http://lists.apple.com/archives/security-announce
BID	http://www.securityfocus.com/bid/
CERT CA	http://www.us-cert.gov/ncas/alerts/
CERT TA	http://www.us-cert.gov/ncas/alerts/
CERT-VN	http://www.kb.cert.org/vuls/
CVE (Common Vulnerabilities and Exposures)	http://web.nvd.nist.gov/view/vuln/search i http://cve.mitre.org/
DEBIAN DSA (Debian Security Announce)	http://www.debian.org/security/
IAVM (Information Assurance Vulnerability Management)	http://iase.disa.mil/index2.html
MANDRAKE MDKSA (Mandrake Security Announce)	http://www.mandriva.com/en/support/security/advisories/
MS (Microsoft Security)	http://technet.microsoft.com/en-us/security/dn481339
MSKB (Microsoft Knowledge Base)	http://support.microsoft.com/
NETBSD	ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/
OSVDB (Open Sourced Vulnerability Database)	http://www.osvdb.org/
OVAL (Open Vulnerability and Assessment Language)	http://oval.mitre.org/find/
REDHAT RHSA (Redhat Security Announce)	http://www.redhat.com/mailman/listinfo/rhsa-announce
SANS	http://www.sans.org/critical-security-controls/
SECTRACK (SecurityTracker)	http://securitytracker.com/
SECUNIA	http://secunia.com/advisories
SGI	ftp://patches.sgi.com/support/free/security/advisories/
SUSE SUSE-SA (SUSE Security Announce)	https://www.suse.com/support/security/advisories/
XF (X-force)	http://xforce.iss.net/

Table 1 Sources that publish vulnerabilities on operating systems

2011, according to which the number of vulnerabilities was 4989[2], which means that almost 95 new vulnerabilities occur every week[3]. The period between publishing vulnerability and applying a patch to a vulnerable program or service on the system is a critical period. The tool used for this

2 This number is based on a large number of sources including mailing lists and recommendations of many producers of programs and equipment,
Source: http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=total_number_of_vulnerabilities

3 Source: http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=total_number_of_vulnerabilities

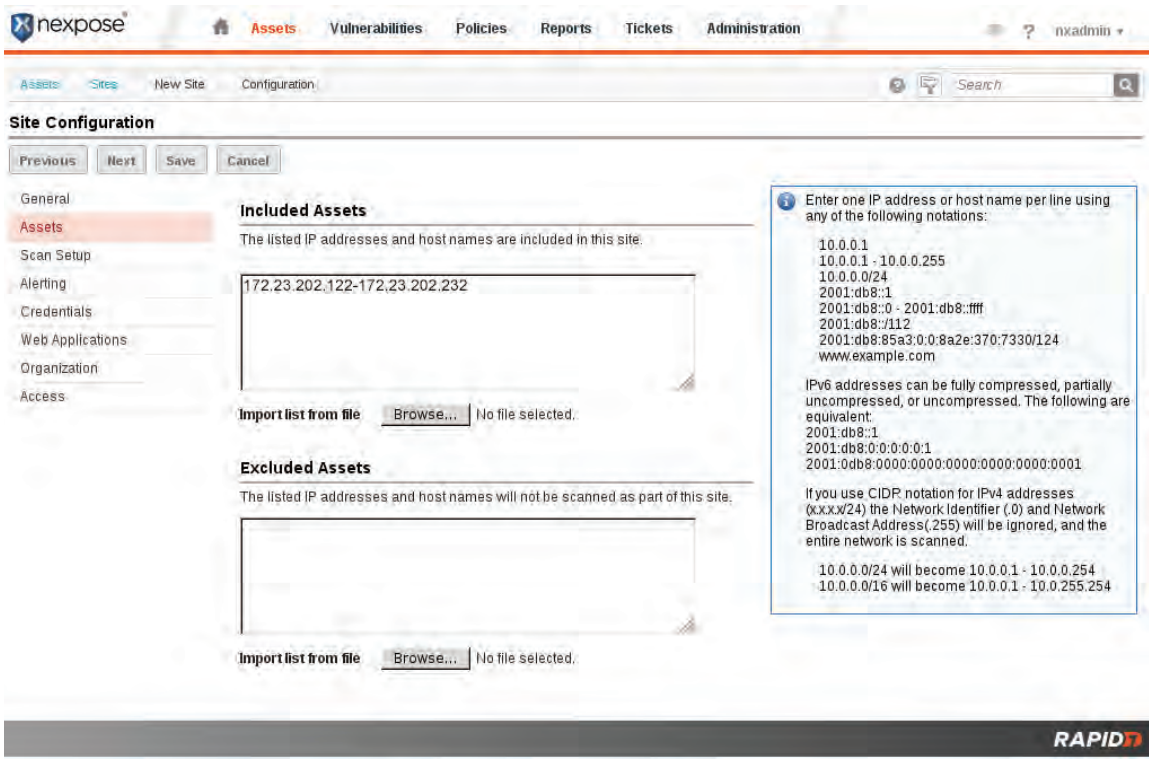


Fig. 1 Preparing the Rapid 7 Nexpose tool for scanning the Linux services

work is called RAPID 7 Nexpose (Fig. 1). The vulnerabilities scan date refers to August 2011 and November 2013 (it is understood that after finalization of this work new vulnerabilities will appear on operating systems and services). With this tool, it is possible to perform planned and selective testing over network services, servers within an organization, and key services in the search for vulnerabilities that can be misused by attackers. In practice, corrective measures are proposed after system scanning. The total number of operating systems covered by this survey is 29 Linux operating systems.

The virtual environment for research purposes with the operating systems shown in the tables (Table 3, Table 4) was realized within the Vmware ESX 5.1.0 platform, the IBM x3650 M3 server and the EMC VNX5300 system, thereby achieving a centralized consolidation of all virtual computer systems intended for testing. Thus a stable platform for effective vulnerability testing with a high level of security was provided.

The virtual environment platform is VMWare ESXi 5.1.0, which is implemented on the IBMx3650 server and the EMC VNX5300 Storage system (Korać 2014).

Server specifications for the IBMx3650 M3:

- 8 CPU Cores (2 x 4C Xeon E5620 80W, 2.4 GHZ 12MB cache
- 56 GB RAM PC3L-10600 ECC DDR3 1333 MHz memory
- 4x IBM 900 GB SAS HDD
- ServeRAID M5014 SAS/SATA controller
- IBM 460W Redundant Power Supply
- IBM UltraSlim Enhanced SATA Multi-Burner

The EMC VNX5300 storage system, with mounted virtual machines for testing purposes, consists of an Intel Xeon 5600 processor, with 16GB cache memory, 8 x 8Gbit FC port, 8 x 1GbE port, 25 x 600GB SAS 15k RPM, 25 x 2TB NL- SAS 7k RPM drives, 5 x 100GB FAST Cache Flash drive, rack cabinet VNX-40U, support for additional capacity expansion, support for CIFS, NFS, iSCSI and FC protocols, Local Protection

VNX5300 CONTROL STATION - EMC RACK
2 x 1GBE DM MODULE 4 PORT FOR VNX5300
VNX5300 ADD ON DM+FC SLIC-EMC RACK
VNX5300 DME: 1 D M+FC SLIC-EMC RACK
VNX5300 DPE; 15X3.5 DRIVES EMC RACK 8X600GB 15K
3 x 3U DAE WITH 15X3.5 INCH DRIVE SLOTS WITH RACK
5 x 100GB FAST CACHE FLSH 15X3.5IN DPE/DAE
17x 600GB 15K SAS DISK DRIVE
VNX 40U RACK WITH CONSOLE
EMC VNX5300 4 PORT 8G FC IO MODULE PAIR
ADDITIONAL 8 G FC SFP FOR VNX 51/53
RACK-40U-60 PWR CORD IEC 309
EMC DOCUMENTATION KIT FOR VNX5300
SECURITY & COMPLIANCE SUITE FOR VNX5300
LOCAL PROTECTION SUITE FOR VNX5300
FAST CACHE FOR VNX5300
BASE FILE LICENSE (CIFS AND FTP) FOR VNX5300
ADV FILE LICENSE (NFS; MPFS AND PNFS) FOR VNX5300
UNISPHERE UNIFIED & VNX OE VNX5300
25 x 2TB 7200RPM 6GB SAS DISK DRIVE
EMC 2ND OPTIONAL SPS
EMC ENHANCED SOFTWARE SUPPORT

Table 2 Specification of the EMC VNX 5300 storage system

Suite licenses, Security & Compliance Suite licenses, redundant power supplies. Table 2 contains a more detailed specification of this system.

The following tables show the operating systems included in vulnerability scanning with the RAPID 7 Nexpose[4] tool:

Table 3 lists the versions of Linux operating systems with added services, the names of the computers with the IP addresses that are included in the scan, by the Rapid7 Nexpose tool.

In the following table (Table 4), services that are additionally hoisted (with default configurations) on Linux operating systems after default installation of the operating system are displayed.

Table 5 shows an overview of the total number of detected vulnerabilities and their relevant sources related to Linux operating systems in 2011 and 2013:

In Table 6 the number of vulnerabilities on Linux OS is presented with detailed review according to severity (Critical – Cr, Serious –Se, Moderate – Mo, Total – To)

The testing was carried out on 29 Linux operating systems. In 2011, 312 unique vulnerabilities were found, and at the level of all scanned Linux

4 https://www.rapid7.com/products/nexpose/

No.	Operating System	Computer Name	IP Address
1.	Mandriva Linux Enterprise Server 5.2 x86	mandriva52enx86	172.23.202.124
2.	Mandriva Linux Enterprise Server 5.2 x64	mandriva52enx64	172.23.202.220
3.	Red Hat Enterprise Linux 4.8 AS x64	rhel48asx64	172.23.202.126
4.	Red Hat Enterprise Linux 4.8 AS x86	rhel48asx86	172.23.202.225
5.	Red Hat Enterprise Linux 5.2 x86	redhat52entx86	172.23.202.194
6.	Red Hat Enterprise Linux 5.2 x64	redhat52entx64	172.23.202.226
7.	Red Hat Enterprise Linux 5.1 x86	redhat51entx86	172.23.202.193
8.	Red Hat Enterprise Linux 5.1 x64	redhat51entx64	172.23.202.227
9.	Red Hat Enterprise Linux 5.6 x64	redhat56entx64	172.23.202.195
10.	Red Hat Enterprise Linux 5.6 x86	redhat56entx86	172.23.202.222
11.	Centos 5.6 x64	centos56x64	172.23.202.196
12.	Centos 5.6 x86	centos56x86	172.23.202.221
13.	Kubuntu 11.04 x86 desktop	kubun1104dskx86	172.23.202.122
14.	Ubuntu 11.04 x64 desktop	ubunt1104dskx64	172.23.202.200
15.	Ubuntu 11.04 x86 desktop	ubunt1104dskx86	172.23.202.230
16.	Ubuntu 11.04 x64 server	ubunt1104srvx64	172.23.202.135
17.	Ubuntu 11.04 x86 server	ubunt1104srvx86	172.23.202.231
18.	Kubuntu 11.04 x86 desktop	kubun1104dskx64	172.23.202.232
19.	Ubuntu 10.04.2 lts x64 server	ubunt1004srvx64	172.23.202.133
20.	Ubuntu 10.04.2 lts x86 server	ubunt1004srvx86	172.23.202.132
21.	Kubuntu 10.04.2 desktop x86	kubun1004dskx86	172.23.202.123
22.	Kubuntu 10.04.2 desktop x64	kubun1004dskx64	172.23.202.229
23.	Debian 60 x86	debian60x86	172.23.202.197
24.	SciLinux 60 x64	sciLinux60x64	172.23.202.199
25.	SciLinux 60 x86	sciLinux60x86	172.23.202.224
26.	Fedora 15 x86	fedora15x86	172.23.202.198
27.	Fedora 15 x64	fedora15x64	172.23.202.223
28.	Slackware 13.37 x86	slackware1337	172.23.202.131
29.	Opensuse 11.4 x86	opensuse1104x86	172.23.202.125

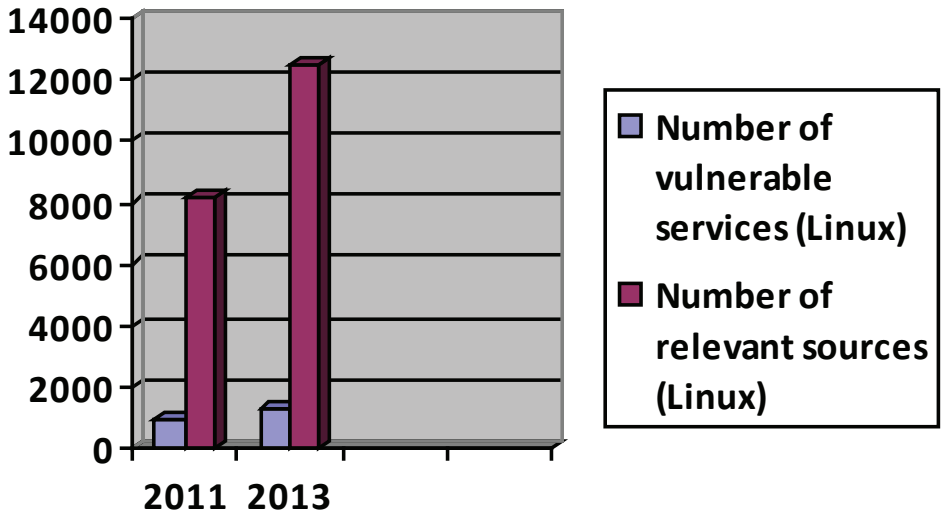
Table 3 Linux operating systems

systems, the total number is 914 vulnerabilities (Table 6, Graph 1). Out of this number, 37 critical, 221 serious and 54 moderate vulnerabilities were found (Graph 2), respectively; considering all scanned systems together 118 critical, 644 serious and 152 moderate vulnerabilities (Table 6) were found. Critical vulnerabilities require emergency intervention. They can be easily abused by a malicious attacker and by their exploitation it is possible to obtain total control over the affected computer system. Serious vulnerabilities are more difficult to exploit and in most cases they can not provide

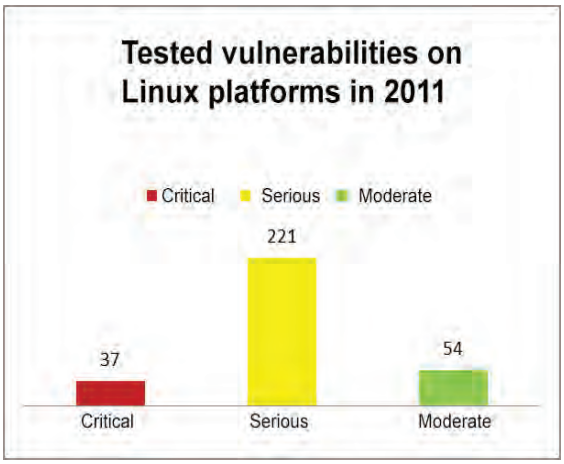
No.	Operating system	IP Address	Added Services
1.	Mandriva Linux Enterprise Server 5.2 x86	172.23.202.124	Apache, PHP, MySql, Tomcat, SSH, FTP, HTTPS
2.	Mandriva Linux Enterprise Server 5.2 x64	172.23.202.220	Apache, PHP, MySql, Tomcat, SSH, FTP, HTTPS
3.	Red Hat Enterprise Linux 4.8 AS x64	172.23.202.126	Apache, PHP, MySql, SSH, FTP, HTTPS
4.	Red Hat Enterprise Linux 4.8 AS x86	172.23.202.225	Apache, PHP, MySql, SSH, FTP, HTTPS
5.	Red Hat Enterprise Linux 5.2 x86	172.23.202.194	Apache, PHP, MySql, SSH, FTP
6.	Red Hat Enterprise Linux 5.2 x64	172.23.202.226	Apache, PHP, MySql, SSH, FTP
7.	Red Hat Enterprise Linux 5.1 x86	172.23.202.193	Apache, PHP, MySql, SSH, FTP
8.	Red Hat Enterprise Linux 5.1 x64	172.23.202.227	Apache, PHP, MySql, SSH, FTP
9.	Red Hat Enterprise Linux 5.6 x64	172.23.202.195	Apache, PHP, MySql, SSH, FTP
10.	Red Hat Enterprise Linux 5.6 x86	172.23.202.222	Apache, PHP, MySql, SSH, FTP
11.	Centos 5.6 x64	172.23.202.196	Apache, PHP, MySql, SSH, FTP
12.	Centos 5.6 x86	172.23.202.221	Apache, PHP, MySql, SSH, FTP
13.	Kubuntu 11.04 x86 desktop	172.23.202.122	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
14.	Ubuntu 11.04 x64 desktop	172.23.202.200	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
15.	Ubuntu 11.04 x86 desktop	172.23.202.230	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
16.	Ubuntu 11.04 x64 server	172.23.202.135	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
17.	Ubuntu 11.04 x86 server	172.23.202.231	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
18.	Kubuntu 11.04 x86 desktop	172.23.202.232	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA

19.	Ubuntu 10.04.2 lts x64 server	172.23.202.133	Apache, PHP, MySql, SSH, FTP, Tomcat, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
20.	Ubuntu 10.04.2 lts x86 server	172.23.202.132	Apache, PHP, MySql, SSH, FTP, Tomcat, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
21.	Kubuntu 10.04.2 desktop x86	172.23.202.123	Apache, PHP, MySql, SSH, FTP, Tomcat, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
22.	Kubuntu 10.04.2 desktop x64	172.23.202.229	Apache, PHP, MySql, SSH, FTP, Tomcat, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
23.	Debian 60 x86	172.23.202.197	Apache, PHP, MySql, SSH, FTP, IMAP, IMAPS, POP, SAMBA
24.	SciLinux 60 x64	172.23.202.199	Apache, PHP, MySql, SSH, FTP
25.	SciLinux 60 x86	172.23.202.224	Apache, PHP, MySql, SSH, FTP
26.	Fedora 15 x86	172.23.202.198	Apache, PHP, MySql, SSH, FTP, NTP
27.	Fedora 15 x64	172.23.202.223	Apache, PHP, MySql, SSH, FTP, NTP
28.	Slackware 13.37 x86	172.23.202.131	Apache, PHP, MySql, SSH, FTP, NTP, SMTP
29.	Opensuse 11.4 x86	172.23.202.125	Apache, PHP, MySql, SSH, FTP

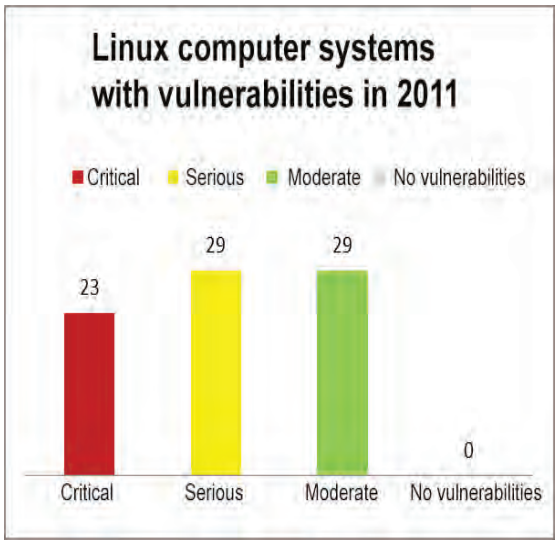
Table 4 Services hoisted on Linux Operating Systems



Graph 1 Presentation of vulnerable services found on Linux OS with the number of relevant sources reporting vulnerabilities in 2011 and 2013



Graph 2 Found vulnerabilities on tested Linux OS in 2011



Graph 3 Number of Linux computing systems by severity of vulnerability in 2011

simultaneous access to the system. When it comes to moderate vulnerabilities, they most often provide information that attackers can use to organize future attacks on computer systems in the network. Moderate vulnerabilities must also be resolved in a timely manner, but they are not as urgent as the previous two. When the computing systems are viewed individually, 118 critical, 644 serious and 152 moderate vulnerabilities were found. Critical vulnerabilities were found in 23 computer systems and they are most susceptible to attack. Serious vulnerabilities were found in 29 computer systems. Moderate vulnerabilities are also present in 29 operating systems (Graph 3). Overview of detected vulnerabilities according to frequency in the examined systems in 2011 is given in Graph 11. None of the tested systems were without vulnerability.

In 2013, 462 unique vulnerabilities were found, and at the level of all scanned Linux systems, the total number is 1307 vulnerabilities (Table 5, Graph 2). Out of this number, 46 critical, 344 serious and 72 moderate vulnerabilities were found (Graph 5). When considering computer systems individually, 149 critical, 953 serious and 205 moderate vulnerabilities were found (Table 6). Critical vulnerabilities were found on 24 computer systems and they are most susceptible to attack. Serious vulnerabilities were found in 29 computer systems. Moderate vulnerabilities are also present on 29 operating systems (Graph 6). Overview of vulnerabilities according to the frequency found on tested systems in 2013 is given in Graph 14. None of the examined systems were without vulnerability.

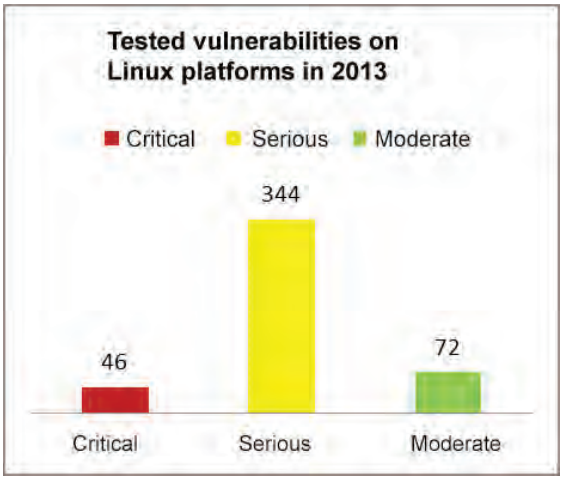
Some services are added on the Linux systems in order to show the actual impact on system vulnerability caused by increasing the number of services. Added services are shown in Table 4. After a default installation and additional services, it can be concluded that none of the tested systems were without vulnerability. Also, there is a noticeable increase in system vulnerability in the period from 2011 to 2013 (Table 6). As can be seen in Graph 15, the critical vulnerabilities increased from 118 to 149, serious vulnerabilities increased from 644 to 953 and moderate increased from 152 to 205.

Significant growth of vulnerability sources has been also noted on Linux operating systems from 8172 to 12456 (Table 6, Graph 1), which shows a significant increase in vulnerability and their abuse in different ways (Korać 2014). The expectation that Linux operating systems after the added services will have a significant increase in the number of vulnerabilities is confirmed and that can be noticed through the growth of critical, serious and moderate vulnerabilities on the system.

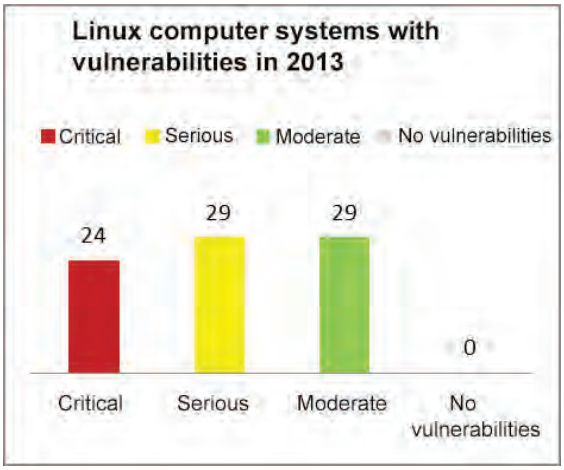
No.	Operating system	IP Address	Number of vulnerabilities in 2011	Number of vulnerabilities in 2013	Difference	No. of sources in 2011	No. of sources in 2013
1.	Mandriva Linux Enterprise Server 5.2 x86	172.23.202.124	43	58	15	314	483
2.	Mandriva Linux Enterprise Server 5.2 x64	172.23.202.220	43	58	15	314	483
3.	Red Hat Enterprise Linux 4.8 AS x64	172.23.202.126	50	56	6	698	801
4.	Red Hat Enterprise Linux 4.8 AS x86	172.23.202.225	50	56	6	698	801
5.	Red Hat Enterprise Linux 5.2 x86	172.23.202.194	47	57	10	599	735
6.	Red Hat Enterprise Linux 5.2 x64	172.23.202.226	47	57	10	599	735
7.	Red Hat Enterprise Linux 5.1 x86	172.23.202.193	47	57	10	599	735
8.	Red Hat Enterprise Linux 5.1 x64	172.23.202.227	47	57	10	599	735
9.	Red Hat Enterprise Linux 5.6 x64	172.23.202.195	45	56	11	578	722
10.	Red Hat Enterprise Linux 5.6 x86	172.23.202.222	45	56	11	578	722
11.	Centos 5.6 x64	172.23.202.196	45	56	11	578	722
12.	Centos 5.6 x86	172.23.202.221	45	56	11	578	722
13.	Kubuntu 11.04 x86 desktop	172.23.202.122	22	39	17	55	210
14.	Ubuntu 11.04 x64 desktop	172.23.202.200	22	39	17	55	210
15.	Ubuntu 11.04 x86 desktop	172.23.202.230	22	39	17	55	210
16.	Ubuntu 11.04 x64 server	172.23.202.135	22	39	17	55	210
17.	Ubuntu 11.04 x86 server	172.23.202.231	22	39	17	55	210
18.	Kubuntu 11.04 x86 desktop	172.23.202.232	22	39	17	55	210
19.	Ubuntu 10.04.2 lts x64 server	172.23.202.133	30	44	14	151	308
20.	Ubuntu 10.04.2 lts x86 server	172.23.202.132	30	44	14	151	308
21.	Kubuntu 10.04.2 desktop x86	172.23.202.123	30	44	14	151	308
22.	Kubuntu 10.04.2 desktop x64	172.23.202.229	30	44	14	151	308
23.	Debian 60 x86	172.23.202.197	23	39	16	99	261
24.	SciLinux 60 x64	172.23.202.199	19	35	16	103	261

25.	SciLinux 60 x86	172.23.202.224	19	35	16	103	261
26.	Fedora 15 x86	172.23.202.198	14	30	16	50	194
27.	Fedora 15 x64	172.23.202.223	14	30	16	50	194
28.	Slackware 13.37 x86	172.23.202.131	11	26	15	53	212
29.	Opensuse 11.4 x86	172.23.202.125	8	22	14	48	185
TOTAL			914	1307	393	8172	12456

Table 5 Linux vulnerabilities and their sources from 2011 and 2013



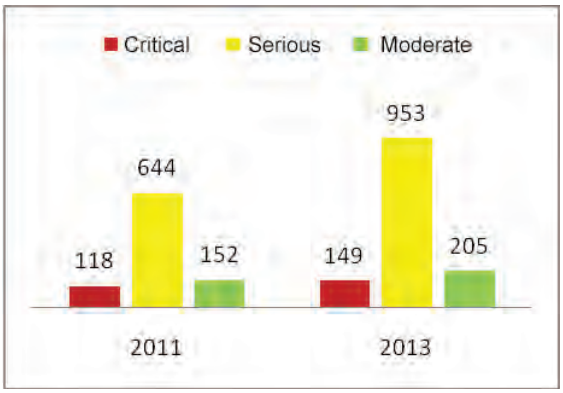
Graph 5 Found vulnerabilities on tested Linux OS in 2013



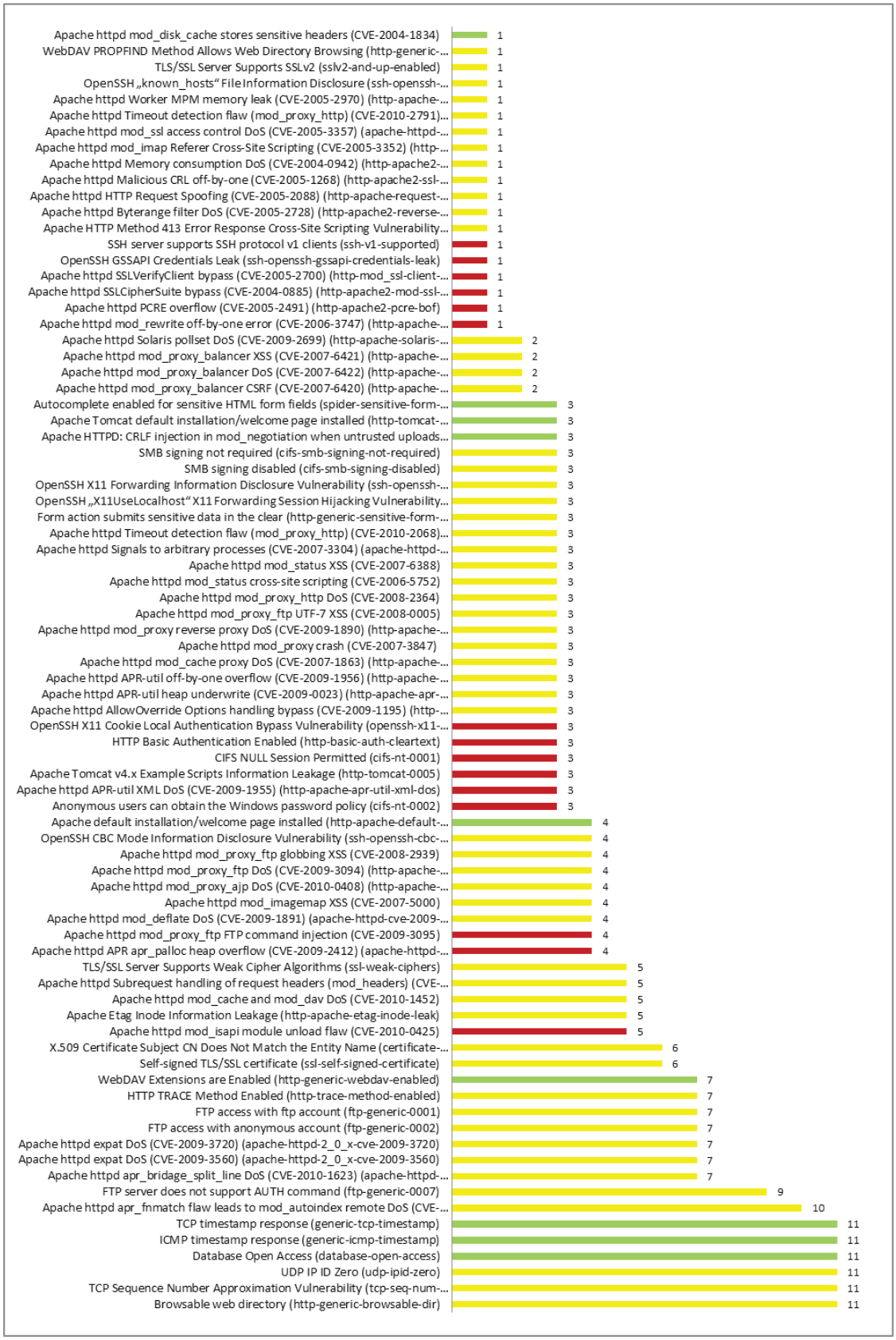
Graph 6 Number of Linux computing systems by severity of vulnerability in 2013

CONCLUSION

The aim of the experimental research in this paper is twofold. On the one hand, vulnerable services that can endanger the security of the system are presented, and on the other, it is possible to apply adequate proactive protection measures. When it comes to protection, it should be noted that there is no unique technology - no silver bullet that can solve all security issues in the organization. If one wants to achieve a certain goal in life, a lot of effort must be made. In this sense, achieving maximum protection is no exception. Implementing an acceptable level of security in an organization depends on the invested resources. By increasing the use of procedural and technical protection measures, the protection of the system and the level of security throughout the organization are increased. As experimental verification the scan of vulnerability of Linux operating systems with the Rapid 7 Nexpose tool was performed. In this way, the vulnerabilities of the Linux operating systems installed by default are presented, with an aim to indicate potential security vulnerabilities. It has been confirmed that after default installations, no computer system is without vulnerabilities. With Linux operating systems after the added services, the number of critical, serious and moderate vulnerabilities on the system is significantly increased as expected.



Graph 8 Global overview of vulnerabilities for all Linux operating systems by years



Graph 4 Overview of found vulnerabilities by frequency in tested systems in 2011 for Linux OS

Graph 7 Overview of found vulnerabilities by frequency on tested systems in 2013 for Linux OS

No.	Operating system	IP Address	Number of vulnerabilities in 2011				Number of vulnerabilities in 2013			
			Cr	Se	Mo	To	Cr	Se	Mo	To
1.	Mandriva Linux Enterprise Server 5.2 x86	172.23.202.124	6	30	7	43	7	40	11	58
2.	Mandriva Linux Enterprise Server 5.2 x64	172.23.202.220	6	30	7	43	7	40	11	58
3.	Red Hat Enterprise Linux 4.8 AS x64	172.23.202.126	10	35	5	50	10	41	5	56
4.	Red Hat Enterprise Linux 4.8 AS x86	172.23.202.225	10	35	5	50	10	41	5	56
5.	Red Hat Enterprise Linux 5.2 x86	172.23.202.194	5	37	5	47	5	46	6	57
6.	Red Hat Enterprise Linux 5.2 x64	172.23.202.226	5	37	5	47	5	46	6	57
7.	Red Hat Enterprise Linux 5.1 x86	172.23.202.193	5	37	5	47	5	46	6	57
8.	Red Hat Enterprise Linux 5.1 x64	172.23.202.227	5	37	5	47	5	46	6	57
9.	Red Hat Enterprise Linux 5.6 x64	172.23.202.195	5	35	5	45	5	45	6	56
10.	Red Hat Enterprise Linux 5.6 x86	172.23.202.222	5	35	5	45	5	45	6	56
11.	Centos 5.6 x64	172.23.202.196	5	35	5	45	5	45	6	56
12.	Centos 5.6 x86	172.23.202.221	5	35	5	45	5	45	6	56
13.	Kubuntu 11.04 x86 desktop	172.23.202.122	4	12	6	22	7	23	9	39
14.	Ubuntu 11.04 x64 desktop	172.23.202.200	4	12	6	22	7	23	9	39
15.	Ubuntu 11.04 x86 desktop	172.23.202.230	4	12	6	22	7	23	9	39
16.	Ubuntu 11.04 x64 server	172.23.202.135	4	12	6	22	7	23	9	39
17.	Ubuntu 11.04 x86 server	172.23.202.231	4	12	6	22	7	23	9	39
18.	Kubuntu 11.04 x86 desktop	172.23.202.232	4	12	6	22	7	23	9	39
19.	Ubuntu 10.04.2 lts x64 server	172.23.202.133	5	19	6	30	7	30	7	44
20.	Ubuntu 10.04.2 lts x86 server	172.23.202.132	5	19	6	30	7	30	7	44
21.	Kubuntu 10.04.2 desktop x86	172.23.202.123	5	19	6	30	7	30	7	44
22.	Kubuntu 10.04.2 desktop x64	172.23.202.229	5	19	6	30	7	30	7	44
23.	Debian 60 x86	172.23.202.197	2	17	4	23	4	30	5	39
24.	SciLinux 60 x64	172.23.202.199	0	15	4	19	0	29	6	35

25.	SciLinux 60 x86	172.23.202.224	0	15	4	19	0	29	6	35
26.	Fedora 15 x86	172.23.202.198	0	10	4	14	0	23	7	30
27.	Fedora 15 x64	172.23.202.223	0	10	4	14	0	23	7	30
28.	Slackware 13.37 x86	172.23.202.131	0	6	5	11	1	18	7	26
29.	Opensuse 11.4 x86	172.23.202.125	0	5	3	8	0	17	5	22
TOTAL			118	644	152	914	149	953	205	1307

Table 6 Number of vulnerable services found on Linux OS classified according to severity

The total number of scanned Linux systems is 29. In this way, vulnerabilities are detected on the system, and then appropriate measures are proposed to overcome the identified security problems.

With proper and regular use of tools for scanning and logging of vulnerabilities on systems, in the presence of a forensic expert, it is possible to get detailed insight into illegal processes in the system and to prevent further illegal activities within a network or a particular computer system. By integrating the results of proactive digital forensics together with systems of preventive protection, detection and analysis of vulnerability, as well as the implementation of multilayer protection architecture (Korać 2010), with timely response to incidental or illegal activities (with a digital forensics specialist), it is possible to increase system security and achieve optimal level protection to an adequately defined security policy.

BIBLIOGRAPHY

Korać, V. 2010
Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja, Arheologija i prirodne nauke, specijalna izdanja, Centar za nove tehnologije, 2010.

Korać, V. 2014
Digitalna forenzika u funkciji zaštite informacionog sistema baziranog na Linux i Windows platformama, unpublished doctoral thesis, Univerzitet u Beogradu, 2014.

REZIME
ISPITIVANJE LINUX SERVISA NA RANJIVOSTI

Alati za analizu ranjivih servisa na sistemu mogu pružiti dragocene informacije o stanju operativnih sistema sa stanovišta zaštite. Istraživanje u ovom radu je obuhvatilo 29 Linux operativnih sistema. Prikupljene informacije obuhvataju veliki broj podataka o prisustvu različitih mrežnih servisa na sistemu koji predstavljaju potencijalne bezbednosne propuste. Na taj način su prezentovane, ranjivosti difoltno instaliranih Linux operativnih sistema (sa pridodatim određenim servisima) sa ciljem ukazivanja na potencijalne bezbednosne ranjivosti. Ove ranjivosti odnosno propusti mogu nastati zbog pogrešno konfigurisanih servisa, poznatih grešaka (eng. Well known bug) u sistemu ili programu, neažuriranosti sistema i njegovih servisa, kao i zbog upotrebe slabe zaštite u konfiguraciji. Cilj ovog ispitivanja jeste da se identifikuju bezbednosni propusti (ranjivi servisi) na difoltno instaliranim Linux sistemima.