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 254104844

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

WINDOWS DEFAULT SERVICES VULNERABILITIES ASSESSMENT

ABSTRACT

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. The research in this paper included 51 Windows 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 Windows operating systems that are installed by default 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or omissions can occur due to incorrectly configured services, well known bugs in the system or program, an outdated system and its services, and the use of poor protection in configuration.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 aim of this assessment is to identify and correct accordingly all recognized security flaws (vulnerable services) on Windows systems installed by default.

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

In the system of protection, vulnerabilities can be in software, hardware, configuration and people (Grubor and Gotić 2012).[1] In this research paper, the focus is on discovering the vulnerability of the operating system software, i.e., operating system services. 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. 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

[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/

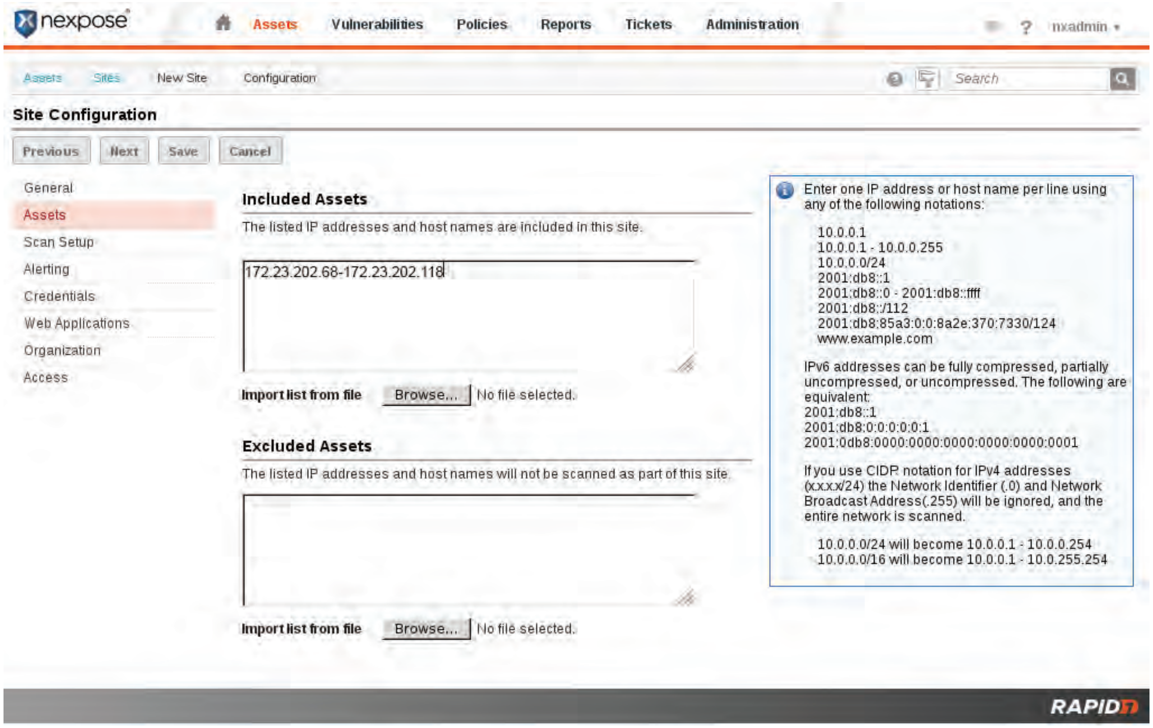
Table 1 Sources that publish vulnerabilities on operating systems

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 and 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 Vulnerability Report for 2011, according to which the number of vulnerabilities was 4989[2], which means that almost 95 new vulnerabilities occur every week [3]. The peri-

[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] ISource: http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=total_number_of_



Site Configuration

Included Assets

The listed IP addresses and host names are included in this site.

172.23.202.68-172.23.202.118

Import list from file Browse... No file selected.

Excluded Assets

The listed IP addresses and host names will not be scanned as part of this site.

Import list from file Browse... No file selected.

Enter one IP address or host name per line using any of the following notations:

```
10.0.0.1
10.0.0.1 - 10.0.0.255
10.0.0.0/24
2001:db8::1
2001:db8::0 - 2001:db8::ffff
2001:db8::/112
2001:db8:85a3:0:0:8a2e:370:7330/124
www.example.com
```

IPv6 addresses can be fully compressed, partially uncompressed, or uncompressed. The following are equivalent:

```
2001:db8::1
2001:db8:0:0:0:0:0:1
2001:0db8:0000:0000:0000:0000:0000:0001
```

If you use CIDR notation for IPv4 addresses (x.x.x.x/24) the Network Identifier (.0) and Network Broadcast Address(.255) will be ignored, and the entire network is scanned.

```
10.0.0.0/24 will become 10.0.0.1 - 10.0.0.254
10.0.0.0/16 will become 10.0.0.1 - 10.0.255.254
```

Fig. 1 Preparation of the Rapid 7 Nexpose tool for scanning of the service

od between publishing a vulnerability and applying a patch to a vulnerable program or service on the system is a critical period. The tool used for this work is called RAPID 7 Nexpose (Figure 1). 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 51 Windows 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 (Figure 2.) and the EMC VNX5300 Storage system.

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

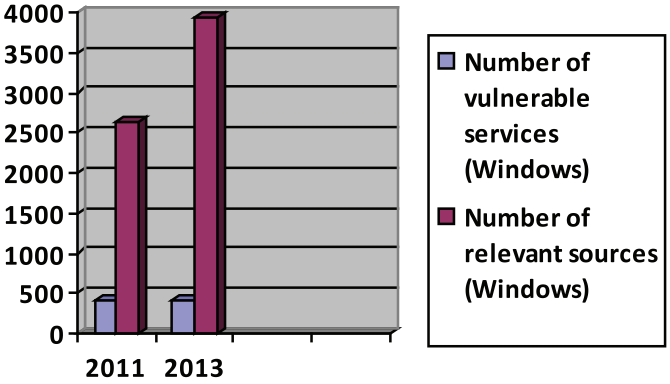
The EMC VNX5300 storage system, with mounted virtual machines for testing purposes, consists of an Intel Xeon 5600 processor, with 16GB cache memory, 8 x 8Gbit FC port, 8 x 1GbE port, 25 x 600GB SAS 15k RPM, 25 x 2TB NL- SAS 7k RPM drives, 5 x 100GB FAST Cache Flash drive, rack cabinet VNX-40U, support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

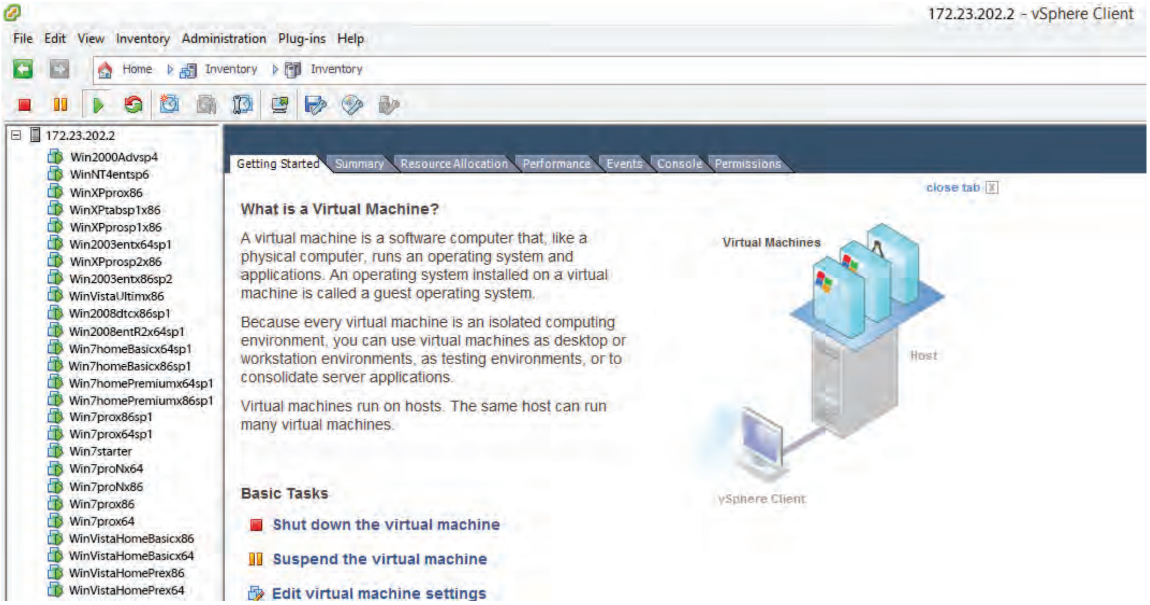
vulnerabilities

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



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


172.23.202.2 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
Getting Started Summary Resource Allocation Performance Events Console Permissions
close tab
Virtual Machines
Host
vSphere Client

172.23.202.2
- Win2000Advsp4
- WinNT4entsp6
- WinXPprox86
- WinXPtabsp1x86
- WinXPprosp1x86
- Win2003entx64sp1
- WinXPprosp2x86
- Win2003entx86sp2
- WinVistaUltimx86
- Win2008dtcx86sp1
- Win2008entR2x64sp1
- Win7homeBasicx64sp1
- Win7homeBasicx86sp1
- Win7homePremiumx64sp1
- Win7homePremiumx86sp1
- Win7prox86sp1
- Win7prox64sp1
- Win7starter
- Win7proNx64
- Win7proNx86
- Win7prox86
- Win7prox64
- WinVistaHomeBasicx86
- WinVistaHomeBasicx64
- WinVistaHomePrex86
- WinVistaHomePrex64

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

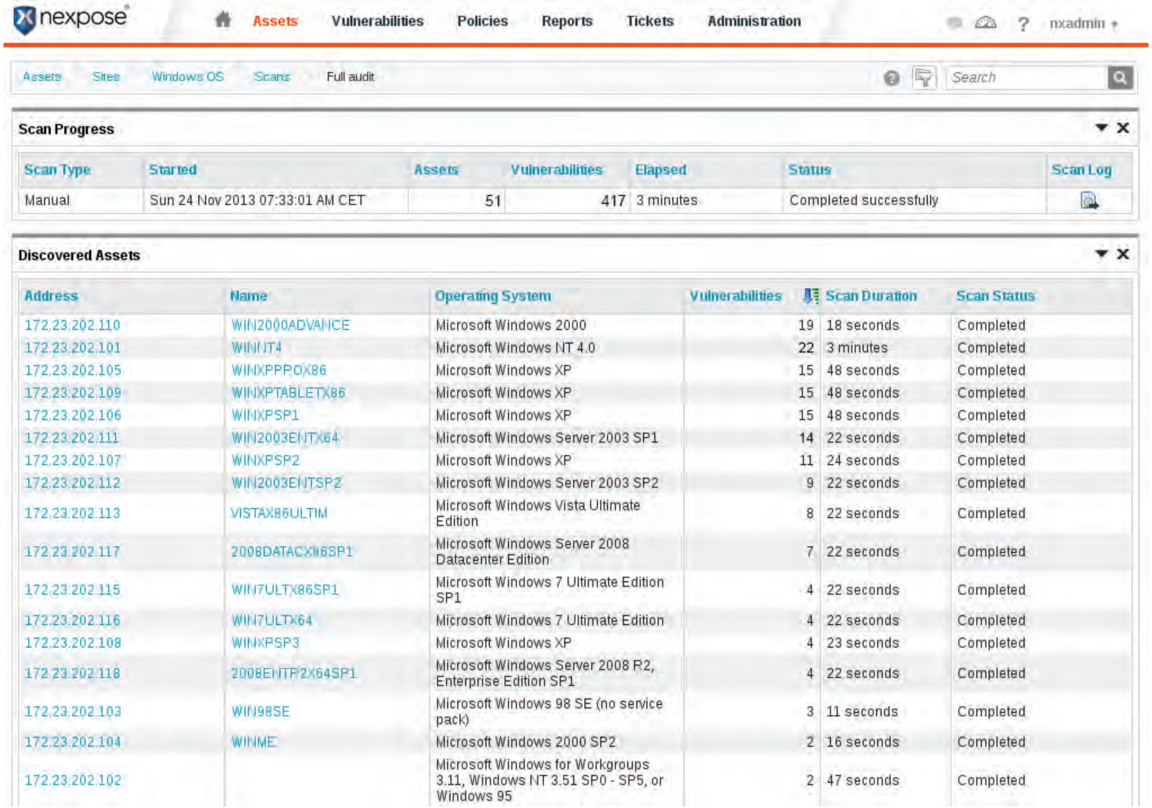
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

- Shut down the virtual machine
- Suspend the virtual machine
- Edit virtual machine settings

Fig. 1 Part of virtual machines prepared for vulnerable systems scanning


nexpose
Assets Vulnerabilities Policies Reports Tickets Administration
nxadmin
Assets Sites Windows OS Scans Full audit
Search

Scan Progress

Scan Type	Started	Assets	Vulnerabilities	Elapsed	Status	Scan Log
Manual	Sun 24 Nov 2013 07:33:01 AM CET	51	417	3 minutes	Completed successfully	

Discovered Assets

Address	Name	Operating System	Vulnerabilities	Scan Duration	Scan Status
172.23.202.110	WIN2000ADVANCE	Microsoft Windows 2000	19	18 seconds	Completed
172.23.202.101	WINNT4	Microsoft Windows NT 4.0	22	3 minutes	Completed
172.23.202.105	WINXPPROX86	Microsoft Windows XP	15	48 seconds	Completed
172.23.202.109	WINXPTABLETX86	Microsoft Windows XP	15	48 seconds	Completed
172.23.202.106	WINXPSP1	Microsoft Windows XP	15	48 seconds	Completed
172.23.202.111	WIN2003ENTX64	Microsoft Windows Server 2003 SP1	14	22 seconds	Completed
172.23.202.107	WINXPSP2	Microsoft Windows XP	11	24 seconds	Completed
172.23.202.112	WIN2003ENTSP2	Microsoft Windows Server 2003 SP2	9	22 seconds	Completed
172.23.202.113	VISTAX86ULTIM	Microsoft Windows Vista Ultimate Edition	8	22 seconds	Completed
172.23.202.117	2008DATACX86SP1	Microsoft Windows Server 2008 Datacenter Edition	7	22 seconds	Completed
172.23.202.115	WIN7ULTX86SP1	Microsoft Windows 7 Ultimate Edition SP1	4	22 seconds	Completed
172.23.202.116	WIN7ULTX64	Microsoft Windows 7 Ultimate Edition	4	22 seconds	Completed
172.23.202.108	WINXPSP3	Microsoft Windows XP	4	23 seconds	Completed
172.23.202.118	2008ENTR2X64SP1	Microsoft Windows Server 2008 R2, Enterprise Edition SP1	4	22 seconds	Completed
172.23.202.103	WIN98SE	Microsoft Windows 98 SE (no service pack)	3	11 seconds	Completed
172.23.202.104	WINME	Microsoft Windows 2000 SP2	2	16 seconds	Completed
172.23.202.102		Microsoft Windows for Workgroups 3.11, Windows NT 3.51 SP0 - SP5, or Windows 95	2	47 seconds	Completed

Fig. 3 Completed Rapid 7 Nexpose tool scanning of vulnerable services on Windows platforms

No.	Operating System	Computer Name	IP Address
1.	Windows nt 4 enterprise sp6	NT4entsp6	172.23.202.101
2.	Windows 95 OSR 2.5	Win95OSR	172.23.202.102
3	Windows 98 se	WIN98SE	172.23.202.103
4.	Windows ME	WINME	172.23.202.104
5.	Windows XP pro x86	WINXPprox86	172.23.202.105
6.	Windows xp pro sp1 x86	WINXPproSP1x86	172.23.202.106
7.	Windows xp pro sp2 x86	WINXPproSP2x86	172.23.202.107
8.	Windows xp pro sp3 x86	WINXPproSP3x86	172.23.202.108
9.	Windows xp tablet pc SP1	WINXPTabX86sp1	172.23.202.109
10.	Windows 2000 advanced server sp4	WIN2000ADVsp4	172.23.202.110
11.	Windows server 2003 Enterprise x64 SP1	WIN2003ENX64sp1	172.23.202.111
12.	Windows Server 2003 Enterprise x86 sp2	WIN2003ENSP2x86	172.23.202.112
13.	Windows Vista ultimate x86	VISTAx86ULT	172.23.202.113
14.	Windows Vista Ultimate SP2 x86	VISTAx86ULTSP2	172.23.202.114
15.	Windows 7 ultimate x86 sp1	WIN7x86ULTSP1	172.23.202.115
16.	Windows 7 ultimate x64	WIN7x64ULT	172.23.202.116
17.	Windows 2008 server datacenter x86 SP1 (kernel as Windows Vista ultim sp2)	2008DTCX86SP1	172.23.202.117
18.	Windows 2008 enterprise x64 server R2 SP1 update June 2011SP1 (kernel as Windows 7)	2008entR2X64SP1	172.23.202.118
19.	Windows 7 Home Basic SP1 x64	WIN7x64HoBaSp1	172.23.202.100
20.	Windows 7 Home Basic SP1 x86	WIN7x86HoBaSp1	172.23.202.99
21	Windows 7 Home Premium SP1 x64	WIN7x64HoPreSp1	172.23.202.98
22.	Windows 7 Home Premium SP1 x86	WIN7x86HoPreSp1	172.23.202.97
23.	Windows 7 Professional SP1 x64	WIN7x64ProSp1	172.23.202.96
24.	Windows 7 Professional SP1 x86	WIN7x86ProSp1	172.23.202.95
25.	Windows 7 starter	WIN7starter	172.23.202.94
26.	Windows 7 Professional N x64	WIN7ProNx64	172.23.202.93
26.	Windows 7 Professional N x86	WIN7ProNx86	172.23.202.92
28.	Windows 7 Professional x64	WIN7Prox64	172.23.202.91
29.	Windows 7 Professional x86	WIN7Prox86	172.23.202.90
30.	Windows Vista Home Basic x86	VISTAx86HoBa	172.23.202.89
31.	Windows Vista Home Basic x64	VISTAx64HoBa	172.23.202.88
32.	Windows Vista Home Premium x86	VISTAx86HoPre	172.23.202.87
33.	Windows Vista Home Premium x64	VISTAx64HoPre	172.23.202.86
34.	Windows Vista Business x86	VISTAx86Bsn	172.23.202.85

35.	Windows Vista Business x64	VISTAx64Bsn	172.23.202.84
36.	Windows Vista Ultimate x64	VISTAx64ULT	172.23.202.83
37.	Windows Vista Home Basic x86 SP2	VISTAx86HoBaSp2	172.23.202.82
38.	Windows Vista Home Basic x64 SP2	VISTAx64HoBaSp2	172.23.202.81
39.	Windows Vista Business x86 SP2	VISTAx86BsnSp2	172.23.202.80
40.	Windows Vista Business x64 SP2	VISTAx64BsnSp2	172.23.202.79
41.	Windows Vista Home Premium x86 SP2	VISTAx86HoPrSp2	172.23.202.78
42.	Windows Vista Home Premium x64 SP2	VISTAx64HoPrSp2	172.23.202.77
43.	Windows 2000 server Sp4	Win2000srv	172.23.202.76
44.	Windows server 2003 Enterprise x86 SP1	WIN2003ENX86sp1	172.23.202.75
45.	Windows server 2003 Standard x86 SP1	WIN2003StX86sp1	172.23.202.74
46.	Windows server 2003 Standard x64 SP1	WIN2003StX64sp1	172.23.202.73
47.	Windows Server 2003 Enterprise x64 SP2	WIN2003ENSP2x64	172.23.202.72
48.	Windows server 2003 Standard x86 SP2	WIN2003StX86sp2	172.23.202.71
49.	Windows server 2003 Standard x64 SP2	WIN2003StX64sp2	172.23.202.70
50.	Windows XP pro sp1 x64	WINXPproSP1x64	172.23.202.69
51	Windows 2008 server Enterprise x86 SP1	2008EntX86SP1	172.23.202.68

Table 3 Windows operating systems

tems included in vulnerability scanning with the RAPID 7 Nexpose[4] tool:

Table 3 lists the versions of Windows operating systems, the names of the computers with the IP addresses that are included in the scan, by the Rapid7 Nexpose tool. By default, Windows operating systems are installed without added services.

Table 4 shows an overview of the total number of detected vulnerabilities and their relevant sources related to Windows operating systems in 2011 and 2013.

In Table 5 the number of vulnerabilities on Windows OS is presented with detailed review according to severity (Critical – Cr, Serious –Se, Moderate – Mo, Total – To)

The testing was carried out on 51 Windows operating system. U 2011, 144 unique vulnerabilities were found, and at the level of all scanned Windows systems, the total number is 414 vulnerabilities (Table 5, Graph 1). Out of this number, 79 critical, 43 serious and 22 moderate vulnerabilities were found (Graph 2.), respectively considering all scanned systems together 211 critical, 117 serious and 86 moderate vulnerabilities were found (Table 5). Critical vulnerabilities require emergency intervention (Korać 2014). They can be relatively easy 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 simultaneous access to the system. Concerning 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 two previously described. As already mentioned, when the computing systems are viewed individually, 211 critical, 117 serious and 86 moderate vulnerabilities were found in total. Critical vulnerabilities were found in a total of 34 computer systems and they are most susceptible to attack

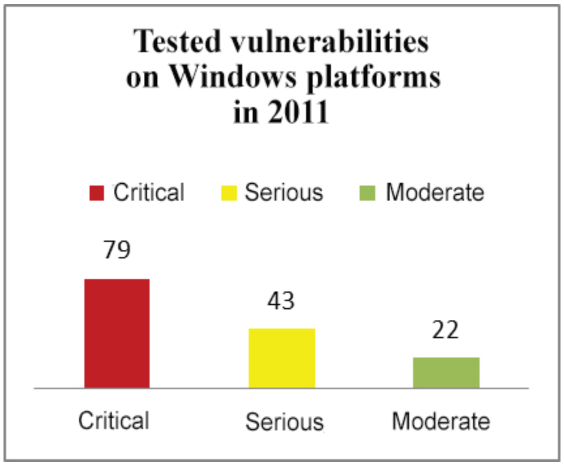
[4] https://www.rapid7.com/products/nexpose/

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 2011**
1.	Windows nt 4 enterprise sp6	172.23.202.101	21	22	1	97	139
2.	Windows 95 OSR 2.5	172.23.202.102	2	2	0	23	27
3	Windows 98 SE	172.23.202.103	3	3	0	22	27
4.	Windows ME	172.23.202.104	2	2	0	23	23
5.	Windows XP pro x86	172.23.202.105	15	15	0	174	247
6.	Windows XP pro sp1 x86	172.23.202.106	15	15	0	174	248
7.	Windows XP pro sp2 x86	172.23.202.107	11	11	0	54	54
8.	Windows XP pro sp3 x86	172.23.202.108	4	4	0	9	10
9.	Windows XP tablet pc SP1 x86	172.23.202.109	15	15	0	174	248
10.	Windows 2000 advanced server sp4	172.23.202.110	18	19	1	225	54
11.	Windows server 2003 Enterprise x64 SP1	172.23.202.111	14	14	0	89	10
12.	Windows Server 2003 Enterprise x86 sp2	172.23.202.112	9	9	0	41	248
13.	Windows Vista ultimate x86	172.23.202.113	8	8	0	53	307
14.	Windows Vista Ultimate SP2 x86	172.23.202.114	7	7	0	24	135
15.	Windows 7 ultimate x86 sp1	172.23.202.115	4	4	0	8	73
16.	Windows 7 ultimate x64	172.23.202.116	4	4	0	8	57
17.	Windows 2008 server datacenter x86 SP1 (kernel as Windows Vista ultim sp2)	172.23.202.117	7	7	0	24	42
18.	Windows 2008 enterprise x64 server R2 SP1 update June 2011SP1 (kerenel as Windows 7)	172.23.202.118	4	4	0	8	8
19.	Windows 7 Home Basic SP1 x64	172.23.202.100	4	4	0	8	8
20.	Windows 7 Home Basic SP1 x86	172.23.202.99	4	4	0	8	42
21	Windows 7 Home Premium SP1 x64	172.23.202.98	4	4	0	8	8

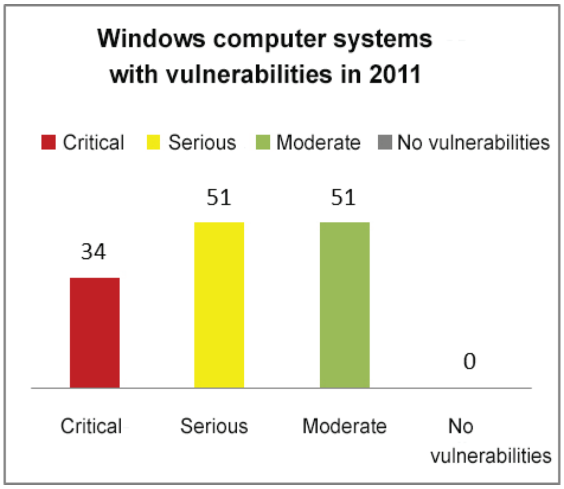
No.	Operating system	IP address	Number of vulnerabilities in 2011	Number of vulnerabilities in 2013	Difference	No. of sources in 2011	No. of sources in 2011
22.	Windows 7 Home Premium SP1 x86	172.23.202.97	4	4	0	8	8
23.	Windows 7 Professional SP1 x64	172.23.202.96	4	4	0	8	8
24.	Windows 7 Professional SP1 x86	172.23.202.95	4	4	0	8	8
25.	Windows 7 starter	172.23.202.94	4	4	0	8	8
26.	Windows 7 Professional N x64	172.23.202.93	4	4	0	8	8
26.	Windows 7 Professional N x86	172.23.202.92	4	4	0	8	8
28.	Windows 7 Professional x64	172.23.202.91	4	4	0	8	8
29.	Windows 7 Professional x86	172.23.202.90	4	4	0	8	8
30.	Windows Vista Home Basic x86	172.23.202.89	8	8	0	53	57
31.	Windows Vista Home Basic x64	172.23.202.88	8	8	0	53	57
32.	Windows Vista Home Premium x86	172.23.202.87	8	8	0	53	57
33.	Windows Vista Home Premium x64	172.23.202.86	8	8	0	53	57
34.	Windows Vista Business x86	172.23.202.85	8	8	0	53	57
35.	Windows Vista Business x64	172.23.202.84	8	8	0	53	57
36.	Windows Vista Ultimate x64	172.23.202.83	8	8	0	53	57
37.	Windows Vista Home Basic x86 SP2	172.23.202.82	7	7	0	24	42
38.	Windows Vista Home Basic x64 SP2	172.23.202.81	7	7	0	24	42
39.	Windows Vista Business x86 SP2	172.23.202.80	7	7	0	24	42
40.	Windows Vista Business x64 SP2	172.23.202.79	7	7	0	24	42
41.	Windows Vista Home Premium x86 SP2	172.23.202.78	7	7	0	24	42
42.	Windows Vista Home Premium x64 SP2	172.23.202.77	7	7	0	24	42
43.	Windows 2000 server Sp4	172.23.202.76	18	19	1	225	307

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 2011
44.	Windows server 2003 Enterprise x86 SP1	172.23.202.75	14	14	0	89	135
45.	Windows server 2003 Standard x86 SP1	172.23.202.74	14	14	0	89	135
46.	Windows server 2003 Standard x64 SP1	172.23.202.73	14	14	0	89	135
47.	Windows Server 2003 Enterprise x64 SP2	172.23.202.72	9	9	0	41	73
48.	Windows server 2003 Standard x86 SP2	172.23.202.71	9	9	0	41	73
49.	Windows server 2003 Standard x64 SP2	172.23.202.70	9	9	0	41	73
50.	Windows XP pro sp1 x64	172.23.202.69	15	15	0	174	248
51	Windows 2008 server Enterprise x86 SP1	172.23.202.68	7	7	0	24	42
TOTAL			**414**	**417**	**3**	**2646**	**3951**

Table 4 Windows vulnerabilities and their sources from 2011 and 2013



Graph 2 Found vulnerabilities on tested Windows OS in 2011

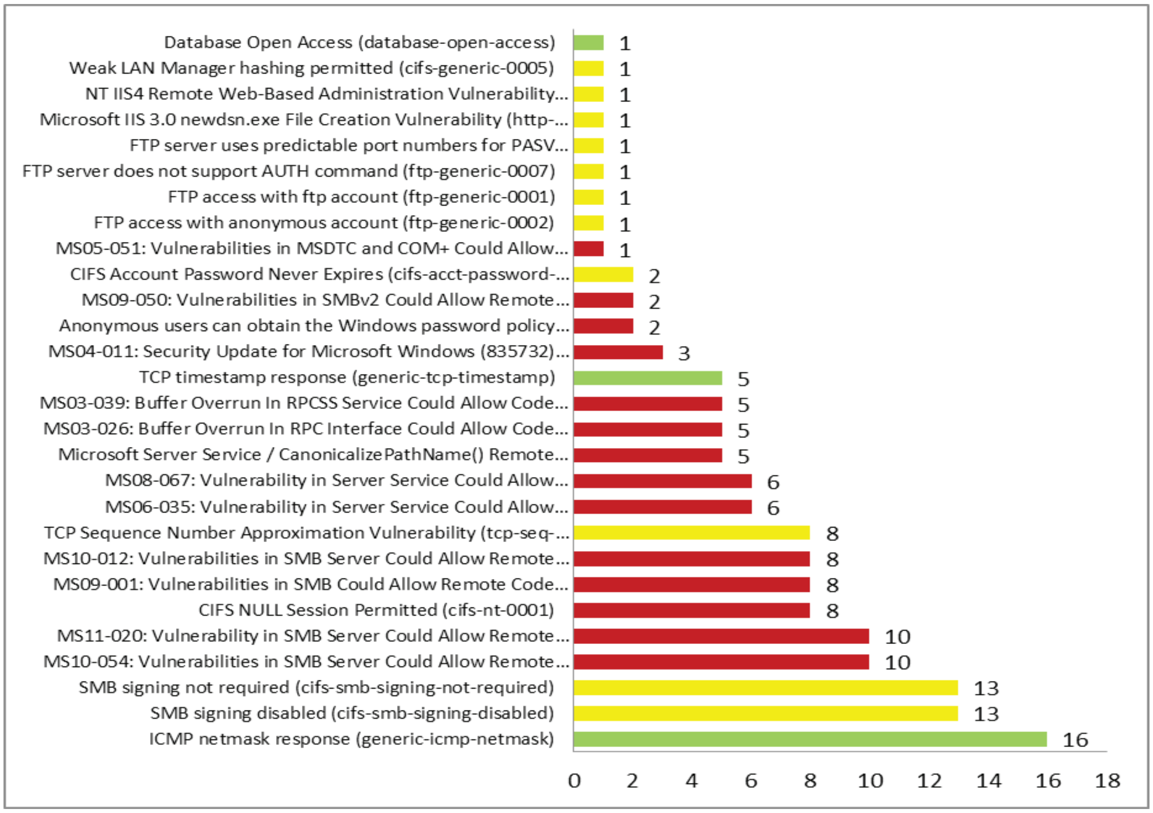


Graph 3 Number of Windows computing systems by severity of vulnerability in 2011

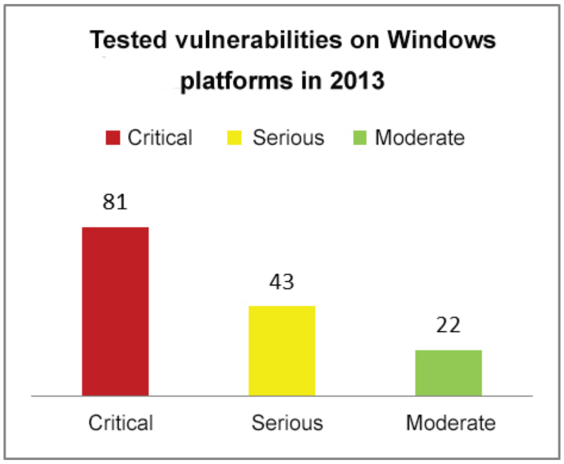
No.	Operating system	IP Address	Number of vulnerabilities in 2011				Number of vulnerabilities in 2013			
			Cr	Se	Mo	To	Cr	Se	Mo	To
1.	Windows nt 4 enterprise sp6	172.23.202.101	9	11	1	21	10	11	1	22
2.	Windows 95 OSR 2.5	172.23.202.102	0	1	1	2	0	1	1	2
3	Windows 98 se	172.23.202.103	0	1	2	3	0	1	2	3
4.	Windows ME	172.23.202.104	0	1	1	2	0	1	1	2
5.	Windows XP pro x86	172.23.202.105	11	3	1	15	11	3	1	15
6.	Windows xp pro sp1 x86	172.23.202.106	11	3	1	15	11	3	1	15
7.	Windows xp pro sp2 x86	172.23.202.107	8	2	1	11	8	2	1	11
8.	Windows xp pro sp3 x86	172.23.202.108	1	2	1	4	1	2	1	4
9.	Windows xp tablet pc SP1	172.23.202.109	11	3	1	15	11	3	1	15
10.	Windows 2000 advanced server sp4	172.23.202.110	13	1	4	18	14	4	1	19
11.	Windows server 2003 Enterprise x64 SP1	172.23.202.111	10	3	1	14	10	3	1	14
12.	Windows Server 2003 Enterprise x86 sp2	172.23.202.112	6	2	1	9	6	2	1	9
13.	Windows Vista ultimate x86	172.23.202.113	4	2	2	8	4	2	2	8
14.	Windows Vista Ultimate SP2 x86	172.23.202.114	3	2	2	7	3	2	2	7
15.	Windows 7 ultimate x86 sp1	172.23.202.115	0	2	2	4	0	2	2	4
16.	Windows 7 ultimate x64	172.23.202.116	0	2	2	4	0	2	2	4
17.	Windows 2008 server Datacenter x86 SP1 (kernel as Windows Vista ultimate sp2)	172.23.202.117	3	2	2	7	3	2	2	7
18.	Windows 2008 enterprise x64 server R2 SP1 update June 2011 (kernel as Windows 7)	172.23.202.118	0	2	2	4	0	2	2	4
19.	Windows 7 Home Basic SP1 x64	172.23.202.100	0	2	2	4	0	2	2	4
20.	Windows 7 Home Basic SP1 x86	172.23.202.99	0	2	2	4	0	2	2	4
21	Windows 7 Home Premium SP1 x64	172.23.202.98	0	2	2	4	0	2	2	4
22.	Windows 7 Home Premium SP1 x86	172.23.202.97	0	2	2	4	0	2	2	4
23.	Windows 7 Professional SP1 x64	172.23.202.96	0	2	2	4	0	2	2	4
24.	Windows 7 Professional SP1 x86	172.23.202.95	0	2	2	4	0	2	2	4
25.	Windows 7 starter	172.23.202.94	0	2	2	4	0	2	2	4
26.	Windows 7 Professional N x64	172.23.202.93	0	2	2	4	0	2	2	4
26.	Windows 7 Professional N x86	172.23.202.92	0	2	2	4	0	2	2	4
28.	Windows 7 Professional x64	172.23.202.91	0	2	2	4	0	2	2	4

No.	Operating system	IP Address	Number of vulnerabilities in 2011				Number of vulnerabilities in 2013			
			Cr	Se	Mo	To	Cr	Se	Mo	To
29.	Windows 7 Professional x86	172.23.202.90	0	2	2	4	0	2	2	4
30.	Windows Vista Home Basic x86	172.23.202.89	4	2	2	8	4	2	2	8
31.	Windows Vista Home Basic x64	172.23.202.88	4	2	2	8	4	2	2	8
32.	Windows Vista Home Premium x86	172.23.202.87	4	2	2	8	4	2	2	8
33.	Windows Vista Home Premium x64	172.23.202.86	4	2	2	8	4	2	2	8
34.	Windows Vista Business x86	172.23.202.85	4	2	2	8	4	2	2	8
35.	Windows Vista Business x64	172.23.202.84	4	2	2	8	4	2	2	8
36.	Windows Vista Ultimate x64	172.23.202.83	4	2	2	8	4	2	2	8
37.	Windows Vista Home Basic x86 SP2	172.23.202.82	3	2	2	7	3	2	2	7
38.	Windows Vista Home Basic x64 SP2	172.23.202.81	3	2	2	7	3	2	2	7
39.	Windows Vista Business x86 SP2	172.23.202.80	3	2	2	7	3	2	2	7
40.	Windows Vista Business x64 SP2	172.23.202.79	3	2	2	7	3	2	2	7
41.	Windows Vista Home Premium x86 SP2	172.23.202.78	3	2	2	7	3	2	2	7
42.	Windows Vista Home Premium x64 SP2	172.23.202.77	3	2	2	7	3	2	2	7
43.	Windows 2000 server Sp4	172.23.202.76	13	4	1	18	14	4	1	19
44.	Windows server 2003 Enterprise x86 SP1	172.23.202.75	10	3	1	14	10	3	1	14
45.	Windows server 2003 Standard x86 SP1	172.23.202.74	10	3	1	14	10	3	1	14
46.	Windows server 2003 Standard x64 SP1	172.23.202.73	10	3	1	14	10	3	1	14
47.	Windows Server 2003 Enterprise x64 SP2	172.23.202.72	6	2	1	9	6	2	1	9
48.	Windows server 2003 Standard x86 SP2	172.23.202.71	6	2	1	9	6	2	1	9
49.	Windows server 2003 Standard x64 SP2	172.23.202.70	6	2	1	9	6	2	1	9
50.	Windows XP pro sp1 x64	172.23.202.69	11	3	1	15	11	3	1	15
51	Windows 2008 server Enterprise x86 SP1	172.23.202.68	3	2	2	7	3	2	2	7
TOTAL			**211**	**117**	**86**	**414**	**214**	**120**	**83**	**417**

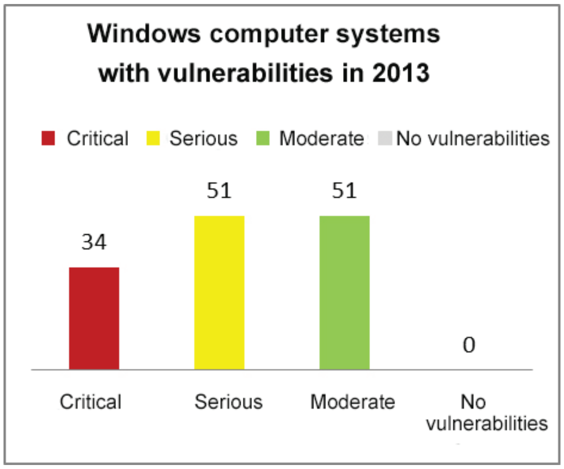
Table 5 Number of vulnerable services on Windows OS classified according to severity



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



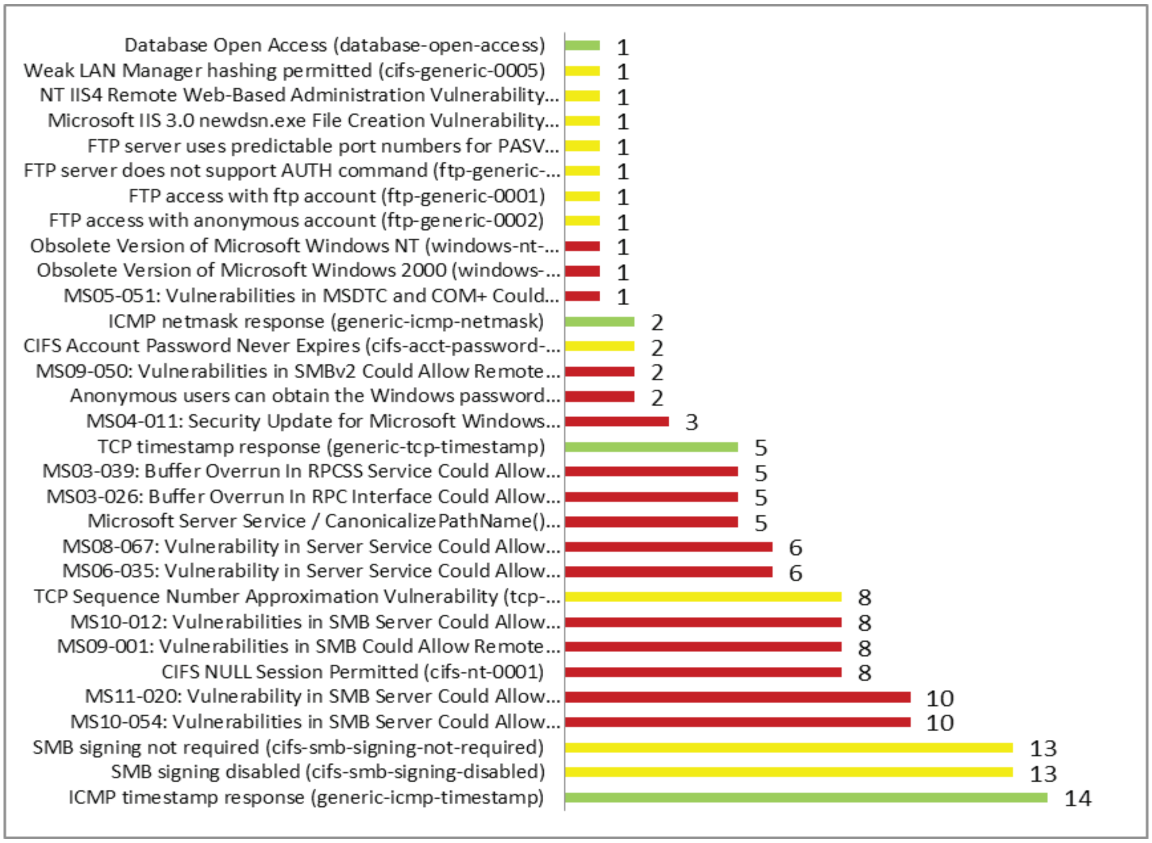
Graph 5. Found vulnerabilities on tested Windows OS in 2013



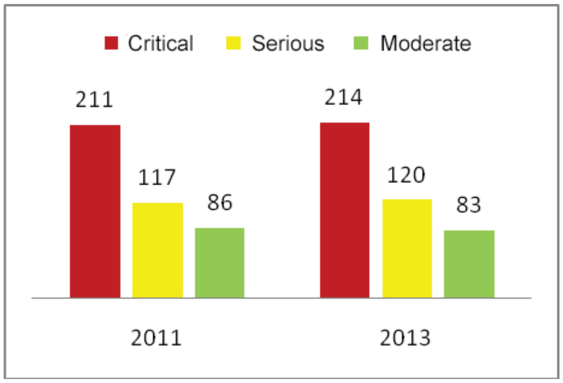
Graph 6 Number of Windows computer systems by severity of vulnerability in 2013

(Graph 3.). Serious vulnerabilities were found in a total of 51 computer systems. Moderate vulnerabilities are also present in 51 operating systems. The presentation of detected vulnerabilities according to frequency in the examined systems in 2011 is given in Graph 4. Although no additional services have been added after the default installation, it can be concluded that none of the tested systems were without vulnerability.

In 2013, 146 unique vulnerabilities were found, and at the level of all scanned Windows systems, the total number is 417 vulnerabilities (Table 5, Graph 1, Figure 3). Out of this number, 81 critical, 43 serious and 22 moderate vulnera-



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



Graph 8 Global overview of vulnerabilities for all Windows operating systems by year

bilities were found (Graph 5). When considering computer systems individually, 214 critical, 120 serious and 83 moderate vulnerabilities were found. Critical vulnerabilities were found on 34 computer systems and they are most susceptible to attack. Serious vulnerabilities were found in 51 computer systems (Graph 6.). Moderate vulnerabilities are also present on 51 operating systems (Graph 6). The presentation of detected vulnerabilities according to frequency in the examined systems in 2013 is given in Graph 7. Although no additional services have been added after the default installation, it can be concluded that none of the tested systems were without vulnerability.

As presented above it can be concluded that all scanned systems are vulnerable, but there has been no significant increase of vulnerability in the period between 2011 and 2013 (as for the scanned Windows operating systems without installed additional services, see Graph 8). Significant growth of vulnerability sources has been also noted on Windows operating systems from 2646 to 3951 (Table 4, Graph 1). Given that no significant increase of vulnerability has been recorded, while a significant growth of the sources of vulnerabilities has been reported, it can be concluded that the existing vulnerabilities have been misused in various ways.

CONCLUSION

The importance and development of new technologies for business modernization and data transfer are constantly increasing. Unfortunately, illegal activities are spreading at the same time. The problem of computer crime is a complex phenomenon. Since the perpetrators of such acts have the necessary knowledge and use sophisticated techniques for their execution, it is all the more difficult to trace and undoubtedly prove the elements of the criminal offence.

The vulnerability scanning of Windows operating systems has been performed with the *Rapid 7 Nexpose* tool. The aim of this experimental research is actually 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 based on the recognized vulnerabilities. It has been confirmed that after default installations there is no computer system without vulnerability.

The total number of scanned Windows operating systems is 51. In this way, the vulnerabilities of Windows operating systems installed by default are presented, with an aim to indicate potential security vulnerabilities, as well as adequate preventive measures for system protection.

With proper and regular use of tools for scanning and logging vulnerabilities on systems, 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 by implementing 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 an optimal level of protection which is suitable to a defined security policy.

Since this topic covers vulnerability scanning technology on Windows operating systems, this work is exceptionally applicable and useful for researchers, students in these fields, computer system administrators, legal and social experts, as well as experts in criminal justice.

BIBLIOGRAPHY

Grubor, G. and Gotić, A. 2012
Korporativna aktivna digitalna forenzička istraga primenom Backtrack – a, 10. Međunarodni naučni skup Sinergija 2012. Univerzitet Sinergija, 2012.

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 WINDOWS DIFOLTNIH SERVISA NA RANJIVOSTI

Upotrebom alata za analizu ranjivih servisa na sistemu moguće je dobiti dragocene informacije o sistemu i mreži sa stanovišta zaštite. Istraživanjem je obuhvaćeno 51 Windows 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 Windows operativnih sistema 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 zaš-

tite u konfiguraciji. Cilj ovog ispitivanja jeste da se identifikuju i na osnovu toga koriguju svi prepoznati bezbednosni propusti (ranjivi servisi) na difoltno instaliranim Windows sistemima.