Modern Windows Operating Systems Vulnerabilities

Theodoros Arambatzis, Ioannis Lazaridis and Sotirios Pouros
AMC Metropolitan College
14th El. Venizelou Str., 54624, Thessaloniki, Greece
t.arambatzis@outlook.com

ABSTRACT

This paper presents the comparison and analysis of vulnerabilities in modern Windows operating systems. Modern tools available on the Internet have been used in order to provide evidence regarding vulnerabilities in most Windows OS including Windows XP and 10. Two scanning methods are realized with three vulnerability scanners. Results derived from measurement comparisons, present the capabilities of each scanner exposing the plethora of vulnerabilities and the effectiveness of the released service packs patching the operating systems' flaws. A comparison between different vulnerability scanners is introduced and conclusions are presented.

KEYWORDS

Vulnerability Assessment, Vulnerability Scanning, Nessus, Nexpose, OpenVAS, Windows, Operating System, Vulnerability Scanner

1 INTRODUCTION

Vulnerability assessment includes the identification, definition, quantification, classification and prioritization of security flaws (vulnerabilities) in a computer infrastructure or a generic computer system. A vulnerability assessment focuses on the impact of a risk in a computer system and moreover, on the impact the object has within the system's existence. In addition, vulnerability assessment endeavors itself with the prospect of diminishing the bearing consequences of the system's object. Furthermore, an assessment can predict the capability of suggested countermeasures and weigh their substantial capability after thoroughly tested, for example perform penetration tests and exploit the vulnerabilities found [1-8].

A vulnerability scanning initiates through the use of dedicated software, widely known as vulnerability scanner. It is an automated process that occurs in computer systems which are connected with each other in a network environment. The vulnerability scanners operate by using a database which contains information regarding well known vulnerabilities. They open TCP/UDP ports, define malware sensitivity level and even attempt to detect misconfigured security settings. Moreover, the software attempt to audit the system's reaction to previously found vulnerabilities and at the end they form a report containing the whole process in detail including the results of the assessment for the security manager to evaluate [9-13].

2 METHODOLOGY

Since the purpose of this paper is to provide practical results of vulnerabilities from some of the most used Windows operating systems in the world, ranging from small companies to large organizations, the methods are practicing a real life scenario and not a generic one [14]. The practicality lies within the fact that the assessment took place with three different widely known vulnerability scanners, which are available for free across the Internet.

2.1 Operating Systems

The aforementioned operating systems that participated in the vulnerability assessment include Technical Previews of Windows 10 and Service Pack 4 for Windows XP. The latter is unofficial, but it was included due to its importance. More specifically, the investigated operating systems are listed in the table below.

Table 1. Windows Operating Systems

Windows OS	Service Packs	Architecture
XP Pro	0, 1, 2, 3, 4	x64
Vista Ultimate	0, 1, 2	x64
7 Starter	0, 1	x32
7 Ultimate	0, 1	x64
8 Pro	-	x64
8.1 Pro	-	x64
10 Pro Insider 10130	-	x64
10 Pro Insider 10147	-	x64
10 Pro	-	x64

2.2 Vulnerability Scanners

The vulnerability scanners used are programs which are available for free. Therefore, the three vulnerability scanners [15-18] are listed in the table below.

Table 2. Vulnerability Scanners

Distributor	Name	Version	Edition
Tenable	Nessus	6.3.7 x64	Home
Rapid7	Nexpose	5.15.1 x64	Community
Open Source	OpenVAS	8 x64	-

2.3 Workbench

The vulnerability assessment has been implemented through the use of two personal computers, one operating with Kali Linux [19] and one having VMware Workstation [20] installed in Windows.
One of the personal computers is a notebook and has the following specifications:

- Fujitsu AH530/HD6 Machine
- Intel Core i5 460M @2.53GHz Processor
- 8GB DDR3 1066MHz System Memory
- Kali Linux 1.1.0a x64 Operating System

Within Kali Linux 1.1.0a, the aforementioned vulnerability scanners were installed (Nessus, Nexpose and OpenVAS). The second computer was a desktop with the following specifications:

- Intel Core i7 4790K @4GHz Processor
- 16GB DDR3 1600MHz System Memory
- Windows 8.1 Pro x64 Operating System

Within Windows 8.1 Pro, VMware Workstation 11 was installed. This program provides the capability of loading an image file containing an operating system. The two computers were operating in the same local network, as they normally would if a security manager was to implement a vulnerability assessment in a computer system of company or an organization.

2.4 Implementation

Initially, two licenses were acquired in order to install Nessus and Nexpore respectively, while OpenVAS was already preinstalled in a Kali Linux environment. While adjusting the appropriate settings for each vulnerability scanner, a bootable image containing an operating system was loaded with specific settings. These settings were: one processor, variable amount of RAM ranging from 1GB to 4GB, variable amount of storage ranging from 40GB to 80GB and bridged network connection, so that the guest operating system would not load on a different network, rather than the host's local network. Once the operating system was fully virtually installed with adequate virtual hardware available, a very specific move had to be made, to disable the

firewall of each operating system and to use the "ipconfig" command in the command prompt in order to display the IPv4 address.

The firewall had to be disabled for the vulnerability scanners to operate as expected, since the first action each scanner does is to send an ICMP "Echo request" and "Echo reply", as known as the ping utility. This kind of action, to temporary disable the firewall is very common in a vulnerability assessment, as long as it is being performed under full control and awareness.

For every vulnerability scanner, two scanning phases were appointed, a basic scan and an advanced scan. The basic scan was different amongst the scanners, due to the different settings approach of a basic scan. Therefore, all three applications had to have their settings tuned, in order to scan a target the same way possible. The advanced scan has every possible setting included for the conduction of the scan. At the end of every scan, a report was being generated and stored, having totally six reports for every operating system - three for a basic scan and three for an advanced scan.

3 RESULTS

The number of vulnerabilities detected in each operating system is listed in the tables below. Most windows operating systems are of an x64 architecture except the Windows 7 Starter OS which is an x32 architecture.

Table 3 depicts many critical vulnerabilities found mostly in Windows XP Pro operating systems, making service pack 3 a very crucial asset to Windows XP's security. Few critical vulnerabilities were discovered in Windows Vista Ultimate and Windows 7 Ultimate. Nessus's basic scan did not manage to address any vulnerabilities in Windows 8.1 Pro or any major in Windows 10 Pro Technical Previews.

Table 3. Number of Vulnerabilities Found with Nessus, Basic Scan

Windows	Nessus Home - Basic Scan				
	Total	Low	Medium	High	Critical
XP Pro	18	0	3	2	13
XP Pro SP1	18	1	3	1	13
XP Pro SP2	9	1	2	1	5
XP Pro SP3	4	1	2	0	1
XP Pro SP4	3	0	2	0	1
Vista Ultimate	3	0	1	0	2
Vista Ultimate SP1	3	0	1	0	2
Vista Ultimate SP2	2	0	1	0	1
7 Starter	2	0	1	0	1
7 Starter SP1	2	0	1	0	1
7 Ultimate	1	0	1	0	0
7 Ultimate SP1	2	0	1	0	1
8 Pro	1	0	1	0	0
8.1 Pro	0	0	0	0	0
10 Pro Insider 10130	1	0	1	0	0
10 Pro Insider 10147	1	0	1	0	0
10 Pro	1	0	1	0	0

Table 4. Number of Vulnerabilities Found with Nessus, Advanced Scan

Windows	Nessus Home - Advanced Scan				
	Total	Low	Medium	High	Critical
XP Pro	18	0	3	2	13
XP Pro SP1	18	1	3	1	13
XP Pro SP2	9	1	2	1	5
XP Pro SP3	4	1	2	0	1
XP Pro SP4	3	0	2	0	1
Vista Ultimate	3	0	1	0	2
Vista Ultimate SP1	3	0	1	0	2
Vista Ultimate SP2	2	0	1	0	1
7 Starter	2	0	1	0	1
7 Starter SP1	2	0	1	0	1
7 Ultimate	1	0	1	0	0
7 Ultimate SP1	2	0	1	0	1
8 Pro	1	0	1	0	0
8.1 Pro	6	0	6	0	0
10 Pro Insider 10130	1	0	1	0	0
10 Pro Insider 10147	1	0	1	0	0
10 Pro	1	0	1	0	0

As shown in table 4, the difference between Nessus basic and advanced scan can be seen in the vulnerabilities discovered in Windows 8.1 Pro in which, Nessus's advanced scan managed to discover six medium vulnerabilities.

Table 5. Number of Vulnerabilities Found with OpenVAS, Basic Scan

Windows	OpenVAS - Basic Scan			
	Total	Low	Medium	High
XP Pro	2	0	2	0
XP Pro SP1	2	0	2	0
XP Pro SP2	0	0	0	0
XP Pro SP3	0	0	0	0
XP Pro SP4	0	0	0	0
Vista Ultimate	2	0	2	0
Vista Ultimate SP1	2	0	2	0
Vista Ultimate SP2	2	0	2	0
7 Starter	2	0	2	0
7 Starter SP1	2	0	2	0
7 Ultimate	2	0	2	0
7 Ultimate SP1	2	0	2	0
8 Pro	2	0	2	0
8.1 Pro	2	0	2	0
10 Pro Insider 10130	2	0	2	0
10 Pro Insider 10147	2	0	2	0
10 Pro	2	0	2	0

Table 5 presents the results of OpenVAS's basic scan results. OpenVAS managed to discover very few critical vulnerabilities in every Windows operating system and it was unable to discover basic vulnerabilities in the Windows XP Pro.

Table 6. Number of Vulnerabilities Found with OpenVAS, Advanced Scan

Windows	OpenVAS - Advanced Scan			
	Total	Low	Medium	High
XP Pro	5	1	3	1
XP Pro SP1	3	0	2	1
XP Pro SP2	2	1	0	1
XP Pro SP3	1	1	0	0
XP Pro SP4	1	1	0	0
Vista Ultimate	3	1	2	0
Vista Ultimate SP1	4	2	2	0
Vista Ultimate SP2	4	2	2	0
7 Starter	4	2	2	0
7 Starter SP1	4	2	2	0
7 Ultimate	5	2	3	0
7 Ultimate SP1	3	1	2	0
8 Pro	4	2	2	0
8.1 Pro	5	2	3	0
10 Pro Insider 10130	5	1	4	0
10 Pro Insider 10147	5	1	4	0
10 Pro	4	1	3	0

On the other hand, OpenVAS advanced scan was able to discover more vulnerabilities, as can be seen in table 6. Thus, the increase of the amount of the vulnerabilities is mostly due to the low and medium vulnerabilities found. Only three critical vulnerabilities were found overall, in the native and first two service packs of Windows XP Pro. Finally, OpenVAS did not manage to compare to Nessus functionality regarding the discovered vulnerabilities.

Table 7. Number of Vulnerabilities Found with Nexpose, Basic Scan

Windows	Nexpose - Basic Scan			
	Total	Moderate	Severe	Critical
XP Pro	17	3	3	11
XP Pro SP1	17	3	3	11
XP Pro SP2	12	2	2	8
XP Pro SP3	5	2	2	1
XP Pro SP4	6	3	2	1
Vista Ultimate	3	3	0	0
Vista Ultimate SP1	10	3	2	5
Vista Ultimate SP2	8	3	2	3
7 Starter	5	3	2	0
7 Starter SP1	5	3	2	0
7 Ultimate	5	3	2	0
7 Ultimate SP1	5	3	2	0
8 Pro	3	3	0	0
8.1 Pro	5	3	2	0
10 Pro Insider 10130	5	3	2	0
10 Pro Insider 10147	5	3	2	0
10 Pro	5	3	2	0

As shown in table 7, Nexpose's basic scan results are similar to Nessus's basic scan. It discovered almost the same number of vulnerabilities as Nessus did and it surpassed OpenVAS.

Lastly, in table 8, it is shown that Nexpose's advanced scan was able to detect more vulnerabilities than the basic scan did. As expected Nessus is the highest recommended freely available software compared to Nexpose and OpenVAS.

Table 8. Number of Vulnerabilities Found with Nexpose, Advanced Scan

Windows	Nexpose - Advanced Scan			
	Total	Moderate	Severe	Critical
XP Pro	17	3	3	11
XP Pro SP1	17	3	3	11
XP Pro SP2	13	2	3	8
XP Pro SP3	6	3	2	1
XP Pro SP4	6	3	2	1
Vista Ultimate	9	3	2	4
Vista Ultimate SP1	3	3	0	0
Vista Ultimate SP2	8	3	2	3
7 Starter	5	3	2	0
7 Starter SP1	5	3	2	0
7 Ultimate	5	3	2	0
7 Ultimate SP1	5	3	2	0
8 Pro	5	3	2	0
8.1 Pro	3	3	0	0
10 Pro Insider 10130	6	4	2	0
10 Pro Insider 10147	5	3	2	0
10 Pro	5	3	2	0

4 FUTURE WORK

The next steps to take would be to expand the operating systems inventory by adding Windows Server, Linux Desktop and Server distributions and Android operating systems. A similar vulnerability assessment could be performed and as a result, the number and significance of vulnerabilities would possibly increase the target audience to be informed.

5 CONCLUSIONS

As far as security is concerned, these results can lead people in choosing more wisely, which Windows operating system they might choose according to their needs.

The vulnerability assessment amongst Windows operating systems is presented. A practical aspect of this assessment is the fact that it reaches a respectful wide audience that uses Windows operating systems in their workplace or at home. Another practical aspect is that the overall process took effect with the use of free and accessible tools, implying that paid full versions of the tools are likely to be more powerful and discover even more abilities, yet the free versions managed to find these many.

Windows XP Pro users are facing a challenging situation that needs to be resolved as soon as possible. There is a minority of Windows XP Pro users that still use Service Pack 2. As of April 8th, Windows XP are no longer supported; addressing the operating system insecure and unable to support modern hardware, as Nessus informs [21]. Users who still work with Windows XP present themselves as a candy in the eyes of malicious computer users. The least they can do is to enable SMB Signing, as Nessus and Nexpose indicate and instruct [22] [23] and finally to upgrade to Service Pack 3 and tinker with the registry. Users that are still collaborating with Windows XP should resign to the safety of the unofficial Service Pack 4, and be as much cautious as possible. Upgrading software and hardware is a very expensive option to consider, and everyone can understand why some companies or organizations might not want to upgrade their software and hardware in order to succeed Windows XP Pro and welcome some future operating systems. Globally, they are the minority, so they should be really cautious regarding security. Security wise, they will be outdated and they should invest a bit in other security assets, should they not upgrade to future, more secure operating systems. The majority of companies and organizations are upgrading the outdated Windows XP Pro to Windows 7 Ultimate, and very few, to Windows 8 and 8.1, even though Microsoft suggests migrating to Windows 8.1 and 10 [24]. Users that are going to operate computers with Windows 7 Ultimate should feel secure, since Microsoft will be distributing security updates until January 14th, 2020. Yet, as Nessus indicates, Windows 7 users should download updates as they launch to at least patch a Microsoft DNS vulnerability that could allow remote code execution [25]. Moreover, the

SNB Signing hasn't changed to mandatory state from previous versions of windows, so Windows 7 users are advised to switch it to mandatory from disabled, through registry tinkering.

By providing the results of this vulnerability assessment, these specific users have the ability to be fully aware regarding the amount of the security issues each operating system has. As a user upgrades to a newer version of Windows, he or she is less likely to expose himself or herself in an insecure state, as the results advice.

To conclude, Windows operating systems maintain vulnerabilities, from low to critical. Apply service packs or updates as soon as possible and invest reasonably in security.

REFERENCES

[1] J. Vacca, Managing Information Security, Second Edition, London, Elsevier, October 2013.

[2] N. Mansourov, D. Campara, System Assurance, First Edition, London, Elsevier, 2010.

[3] K. Julisch, C. Kruegel, Detection of Intrusion and Malware, and Vulnerability Assessment: Second International Conference, DIMVA 2005, Vienna, Austria, July 2005, Proceedings, Wien, Springer, 2005, pp. 2-20.

[4] T. R. Peltier, J. Peltier, J. A. Blackley, Managing A Network Vulnerability Assessment, First Edition, Boca Raton, Auerbach Publications, May 2003.

[5] J. Vacca, Computer and Information Security Handbook, First Edition, London, Elsevier, July 2009.

[6] T. Holz, H. Bos, Detection of Intrusion and Malware, and Vulnerability Assessment: Eighth International Conference, DIMVA 2011, Amsterdam, The Netherlands, July 2005, Proceedings, New York, Springer, 2005, pp. 2-20.

[7] A. Jones, D. Ashenden, Risk Management for Computer Security, First Edition, London, Elsevier, April 2005.

[8] Á.M. Eduardo and C.V. Alfredo, Vulnerability Assessment of Spatial Networks: Models and Solutions, Combinational Optimazation, Third International Symposium 2014, Houten, Springer, 2014, pp. 433-444.

[9] EC-Counsil, Network Defense: Security and Vulnerability Assessment, First Edition, Boston, Cengage Learning, April 2010.

[10] M. Dowd, J. McDonald, J. Schuh, The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, First Edition, Boston, Addison - Wesley Proffesional, November 2006.

[11] P. S. Anton, R. H. Anderson, R. Mesic, M. Scheiem, Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology, Santa Monica, RAND Corporation, January 2004.

[12] S. Manzuik, A. Gold, C. Gatford, Network Security Assessment: From Vulnerability to Patch, First Edition, Rockland, Syngress, November 2006.

[13] D. Maynor, T. Wilhelm, Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research, First Edition, Rockland, Syngress, October 2007.

[14] T. Jaeger, Operating System Security, California, Morgan & Claypool Publishers, October 2008.

[15] J. Beale, C. van der Walt, R. Deraison, Nessus Network Auditing, First Edition, Rockland, Syngress, October 2004

[16] N. Archibald, G. Ramirez, N. Rathaus, J. Burke, B. Caswell, R. Deraison, Nessus, Snort, & Ethereal Power Tools: Customizing Open Source Security Applications, First Edition, Rockland, Syngress, August 2015

[17] J. Broad, Mastering Nexpose and Metasploit: A Lab-Based Approach to Mastery, First Edition, Rockland, Syngress, November 2015

[18] H. Reibold, OpenVAS kompakt, Saarbrücken, Brain-Media.de, June 2013

[19] D. W. Dieterle, Basic Security Testing with Kali Linux, First Edition, CreateSpace Independent Publishing Platform, January 2014

[20] S. van Vugt, VMware Wosktation - No Experience Necessary, Birmingham, Packt Publishing, August 2013

[21] http://www.tenable.com/plugins/index.php?view=single&id=73182 (last accessed 4th of July 2015)

[22] http://www.tenable.com/plugins/index.php?view=single&id=26920 (last accessed 4th of July 2015)

[23] http://www.hsc.fr/ressources/presentations/null_sessions/ (last accessed 4th of July 2015)

[24] http://windows.microsoft.com/en-us/windows/end-support-help (last accessed 4th of July 2015)

[25] http://www.tenable.com/plugins/index.php?view=single&id=53514 (last accessed 4th of July 2015)