Vulnerability Scanners Capabilities for Detecting Windows Missed Patches: Comparative Study

Mohamed Alfateh Badawy, Nawal El-Fishawy, and Osama Elshakankiry

Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt
mohamed.alfateh@owasp.org, {nelfishawy,osama1975}@hotmail.com

Abstract. Vulnerability scanners are automated tools that define, identify, and classify security holes (vulnerabilities) in a computer, server, network, or communications infrastructure. Scanners discover missed patches on target systems and report related vulnerabilities. Many of the current information security systems use vulnerability scanners as the main part in the risk assessment process. Others depend on the scanners output in the systems patch management. This paper assesses the effectiveness of depending on vulnerability scanners in the information security management system. It compares between four of the leading vulnerability scanners in the market and carries out a study of their effectiveness in detecting missed patches.

The results show the severity of relying on vulnerability scanners to discover system patches status. A number of false positive and false negative detections for the system patches are reported by each of the tested scanners. The severe level for some of the unreported missed patches ranked as critical that puts the system in a high risk and makes it vulnerable for different attacks.

Keywords: Vulnerability scanner, patch management, risk assessment.

1 Introduction

The increasing volume of attacks on the Internet has increased the demand for sophisticated tools and techniques to detect systems vulnerabilities and to perform vulnerability analysis. Minimizing this threat requires organizations to configure systems properly, use the latest software, and install the recommended security updates. Creating and communicating a documented security release and update policy is a vital part of any companys risk-management process [1].

Vulnerability scanning plays a main role to identify systems vulnerabilities during the vulnerability management process. Vulnerability scanners are automated tools that are used to perform system discovery, identify open ports and running services on the discovered system, and then analyze them for potential vulnerabilities. In addition, scanners can help in identifying outdated software versions, missing patches, and misconfigurations [2].

A.I. Awad, A.E. Hassanien, and K. Baba (Eds.): SecNet 2013, CCIS 381, pp. 185–195, 2013.

On the other hand the system patches correct security and functionality problems in software and firmware. From a security perspective, security patches are most often of interest because they are mitigating software flaw vulnerabilities; i.e., applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation.

In enterprise networks, deploying software patches is not an easy task; the deployment should be managed through patch management process. Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems [3].

Agentless scanning using network scanners is one of three techniques introduced by National Institute of Standards and Technology (NIST) to perform patch management in enterprise networks [4]. Moreover, research was introduced enhancing the intrusion detection system based on the vulnerability scanners detections [5].

In this paper, a comparative study is performed to determine to what extent vulnerability scanners could be trusted in detecting missed patches or even in verifying the installation of a specific patch.

Although Gartner generates an annual report to compare vulnerability scanners [6][7], the evaluation criteria are mainly based on the vendors market share and the scanners add-ons features such as integration with other security products, reporting capabilities, deployment options, management features and compliance check.

This paper focuses on the scanners capabilities of detecting Microsoft windows missed patches. In addition, it shows the severity level for the unreported patches. It starts by determining and studying all related patches released from Microsoft. Next, in different system conditions, it performs the scans using each vendor separately. Finally, it compares the scan results with Microsoft windows updates.

The rest of the paper is organised as following. Section 2 describes the vulnerability assessment and vulnerability scanners. Section 3 describes Microsoft update, Section 4 illustrates common security impacts related to Microsoft missed patches. Section 5 presents the experimental results and, finally, Section 5 concludes the paper.

2 Vulnerability Assessment and Vulnerability Scanners

Vulnerabilities are weaknesses in software that may enable an attacker to compromise the integrity, availability, or confidentiality of that software. When the term vulnerability assessment is used in the context of vulnerability scanners it means the process of finding known vulnerabilities in a network [8]. This process identifies vulnerabilities so they can be eliminated before exploited by malicious software or hackers. The vulnerabilities that constitute threats in a network include software defects, unnecessary services, misconfigurations and unsecured accounts.

During network systems lifetime the security must be constantly updated and developed to encounter new and enhanced vulnerabilities. NIST has described

a model for security maintenance. The model recommends using vulnerability scanners among other tools, in regular testing to make sure that the network is secured [9].

A vulnerability scanner starts like a port scanner and tries to identify all the hosts running in the defined IP range. When the hosts have been found, the scanner tries to find all opened ports and corresponding services on all active hosts, and then identifies vulnerabilities in the scanned host. This is done through comparing running operating systems and software applications with known vulnerabilities stored in a database [9]. In some cases, vulnerability is identified from the information of a banner and version test. In other cases, the scanner makes a complete exploitation of the vulnerability to insure its existence.

2.1 Vulnerability Scanners False Alerting

A false-positive is when the vulnerability scanner reports an error that is not present. On the other hand, the false-negative is when the vulnerability scanner missed reporting an existing vulnerability.

There are a number of reasons of why a false alerting occurs. The false alerting may happen because of the technique used to check for vulnerabilities. Some scanners just look for signs such as registry entries in Microsoft Windows operating systems to identify that a specific security patch or update has been implemented. Other scanners look at relevant DLL and other files affected by applying the patch or update. While the latter is slightly slower, it is more accurate and reliable [10].

There are many instances where a Windows operating system can have a security patch seemingly applied, but not actually in effect. For example, there could have been an error during the patch update process or the patch required a reboot to take effect. Moreover, the network connection between the scanner and the vulnerable system might drop some scanning packets and affect the scanner detection. Also, the vulnerable service running on the target system might have become temporarily unavailable during the scanning requests.

Another very important cause of false alerting is the time between when vulnerability is disclosed and when a scanner database is updated. It is very common that vulnerabilities can get reported where the scanner is delayed in updating the scanning database to include checks for those vulnerabilities.

2.2 Tested Vulnerability Scanners

To perform our comparative experiments, we used four of the leader vulnerability scanners on the market. In addition and after each scan, we used Microsoft Baseline Security Analyzer (MBSA) [11] to verify the scanning output. The following is a brief description for the scanners we used.

McAfee Vulnerability Manager. Was formerly known as Foundstone [12]. MVM can be integrated with other McAfee products as well as a large number of third-party security products. In 2011 and 2012, MVM was rated as a strong positive in Gartner report for the vulnerability assessment.

Retina Network Security Scanner. Retina scanner was developed by eEye Digital Security and has been acquired by BeyondTrust in May 2012 [13]. Retina offer a Fix-it feature to automatically correct some system security issues discovered during the scanning including registry settings and file permissions. Retina rated positive in Gartner report.

Nexpose Vulnerability Management from Rapid7. In 2009 Rapid7 acquired the open-source Metasploit framework penetration testing engine, and released a commercial version of it in 2010. Nexpose integrates with Metasploit to validate security risks for the discovered vulnerabilities [14]. The scanner was rated strong positive in Gartner reports.

Nessus Vulnerability Scanner from Tenable. The "Nessus" project was started by Renaud Deraison in 1998 to provide a free remote security scanner to the Internet community. In 2005, Tenable changed Nessus to a proprietary (closed source) license [15]. In 2012 the scanner rated strong positive in Gartner report.

3 Microsoft Update

Microsoft update is a service from Microsoft that provides a listing of Microsoft software updates, drivers, and hotfixes. Microsoft offers important, recommended, and optional updates.

Important updates provide significant benefits such as improved security and reliability. Recommended updates are those enhance the performance and the computing OS experience. Optional updates might include new or updated driver software for a specific device.

A security update is a widely released fix for a product-specific, security-related vulnerability. Microsoft security updates are accompanied by two documents: a security bulletin and a Microsoft knowledge base article. Microsoft schedules the release of the security update and the security bulletin on the second Tuesday of the month at 10:00 AM in the Pacific Time zone. The security bulletin advance notification occurs three business days before this [1].

Microsoft also provides service pack (SP) update. PS is a tested, cumulative set of all hotfixes, security updates, and critical updates.

A single security update often addresses multiple vulnerabilities from the Common Vulnerabilities and Exposures (CVE) database each of which is listed in a corresponding Microsoft security bulletin along with any other relevant issues.

Security vulnerabilities are rated based on their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low. Microsoft evaluates each issue and quantifies an issues impact objectively on a technical level for default configurations. Based on this analysis and the maximum security impact, Microsoft supplies a rating in the security bulletin. Table1 defines the four Microsoft severity ratings and their corresponding impact [1].

Table 1. Microsoft Severity Ratings

Rating	Definition
Critical	A vulnerability whose exploitation could enable the propagation of an Internet worm with little or no user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users data, or of the integrity or availability of processing resources.
Moderate	A vulnerability whose exploitation is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

4 Security Impacts Related to Microsoft Released Patches

Comparing operating system vulnerabilities to non-operating system vulnerabilities require determining whether a particular program or component should be considered part of an operating system. Microsoft update service releases security updates for different Microsoft product like Internet Explorer and Microsoft Office as well as the security updates released for the operating system components.

Microsoft provides information about the availability of Proof-of-Concept (PoC) exploit code or active attacks related to vulnerabilities addressed by Microsoft security updates [1]. The maximum security impact for each released update is mentioned in the Microsoft Security Bulletin. The following are the common Security Impact reported in the Microsoft security bulletin:

- Remote Code Execution
- Denial of Service
- Information Disclosure
- Elevation of Privilege
- Tampering
- Spoofing

5 Comparative Study

In our experiments, we used the latest available version for the tested scanners with a license for each scanner that gave us an access to the latest released scanner database on-time updates. Also, Windows server 2008 was used as the target machine. Table 2 shows the versions for the used scanners.

Table 2. Tested Vulnerability Scanners' Version

Scanner Name	Version
MVM	7.5
Retina	5.18
Nessus	5.0.2
Nexpose	5.5.12

In order to detect the effects of installing SP on the accuracy of the scanning, the test was conducted through two phases. At the first phase, the scans were performed against the target server before installing any updates or SPs. At the second phase the scans was repeated after installing the SP2.

We start our experiments by listing all released Microsoft security updates for windows server 2008 and understand the new patches those replaced older ones.

5.1 First Phase

In this phase, the scans were performed before installing any updates or SP. To verify the scanning output and to detect how often the scanners update their scanning data-base, the scans were performed two times before the Microsoft Tuesday updates and two times after the Microsoft Tuesday updates respectively. In the latter, the first scan was performed one day after disclosing Microsoft updates and the second scan was performed one week later.

By running the scans before Microsoft Tuesday updates, the two results were the same for each scanner. Fig. 1 shows the comparative analysis for the scanners reporting for both false positive and false negative.

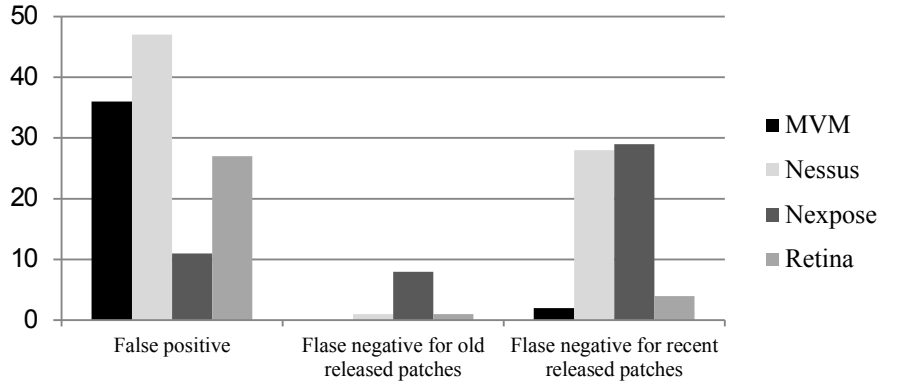

Fig. 1. Vulnerability scanners false positive and negative results before Windows Tuesday update

It is noticed that all the scanners have a higher detection ratio for the old Microsoft patches than the recent released patches. In addition, MVM and Retina were found the only scanners that significantly mentioned Microsoft replacement patches. Nessus has a higher number of false positive detections because of reporting many missed Microsoft patches that were replaced with newer ones.

After Microsoft released the Tuesday updates, the scanners were run two times. (Fig. 2 shows the output results of running the scanners one day after the release of Microsoft updates).

The results show that all scanners except Nexpose had updated their scanning data-base and reported the new released windows updates. The released windows updates include some patches that replaced many of the old Microsoft patches. Also, it is shown that none of the scanner reported the replaced patches, which explains the increase in the false positive.

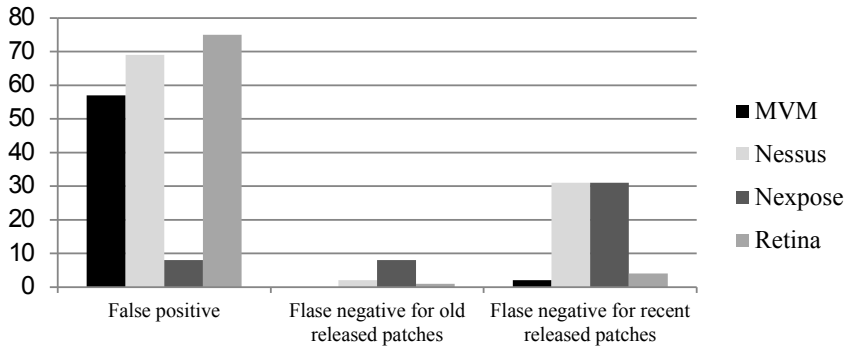

Fig. 2. Vulnerability scanners false positive and negative results before Windows Tuesday update

By performing the scans one week after the patches release date; the only noticeable result was the significant decrease of the false positive reported by MVM scanner. This is because MVM was the only scanner that updates the replaced patches in its reporting; Fig. 3 shows the comparative results for all scanners.

The results of the scans performed in the first phase show the significant effect of misreporting the replaced Microsoft patches, Moreover; the results show some limita-tion for all the scanners in detecting the recent released Microsoft updates rather than the old ones

Table 3 shows the attacks related to the missed patches reported for each of the tested scanners:

Table 4 shows the average severe level for the missed patches reported for the tested scanners

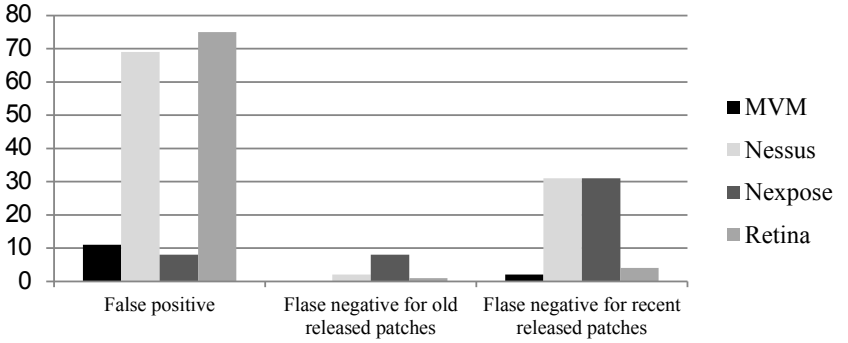

Fig. 3. Vulnerability scanners false positive and negative results before Windows Tuesday update

Table 3. Unreported Patches Related Attacks

	MVM	Nessus	Nexpose	Retina
Remote Code Execution	2	23	25	4
Denial of Service	0	2	2	0
Information Disclosure	0	2	3	1
Elevation of Privilege	0	5	4	0
Tampering	0	0	1	0
spoofing	0	0	1	0
Security Feature Bypass	0	2	2	0

Table 4. Scanners Unreported Patches Severe Level

	MVM	Nessus	Nexpose	Retina
Critical	2	11	12	1
Important	0	15	11	2
Moderate	0	6	8	2
Information	0	0	2	0

5.2 Second Phase

In this phase, the scanners were used to scan the same machine after installing SP2, and the latest dotNet framework version. Again, the scans were performed twice; before Microsoft released the Tuesday update and after.

The comparative result for the scanners before Microsoft Tuesday patch updates is shown in Fig. 4.

The results show that after installing the SP2 all scanners were able to detect most of the missed patches. The increase of the false positive for MVM scanner was due to incorrect reporting for some replaced patches. In addition MVM was the only scanner that exactly reported all the replaced patches, Retina reported some of them, and both Nessus and Nexpose did not report any.

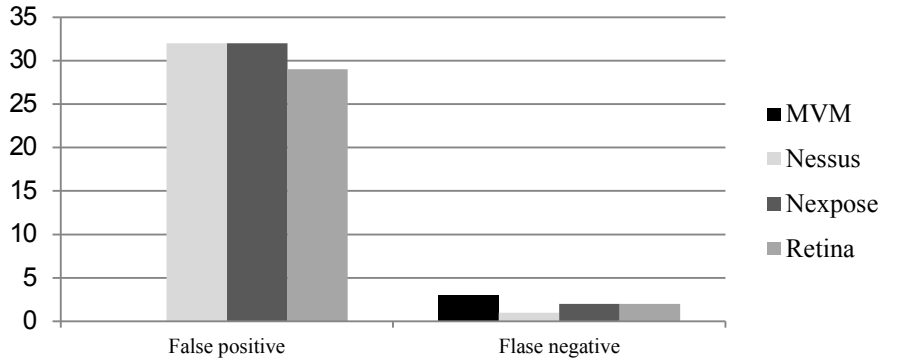

Fig. 4. Vulnerability scanners false positive and negative results before Windows Tuesday update

The scans were repeated one day after the releasing of the new Microsoft Tuesday patches, Fig. 5 shows the results for each scanner.

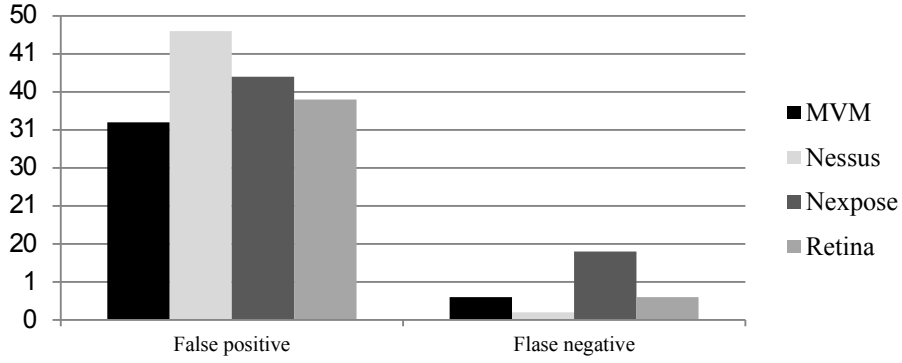

Fig. 5. Vulnerability scanners false positive and negative results before Windows Tuesday update

The results show that all scanners except Nexpose updated their scanning database and reported the new released patches; however, the increase of the false positive for MVM scanner were due to that some new release patches replaced old ones and MVM did not update the replaced patches.

Table 5 shows the attacks related to the missed patches reported for each of the tested scanners.

Table 6 shows the average severe level for the missed patches reported for the tested scanners.

Table 5. Second Phase Unreported Patches Related Attacks

	MVM	Nessus	Nexpose	Retina
Remote Code Execution	3	1	5	2
Denial of Service	0	0	1	0
Elevation of Privilege	0	0	3	1

Table 6. Second Phase Scanners Unreported Patches Severe Level

	MVM	Nessus	Nexpose	Retina
Critical	3	1	3	1
Important	0	0	5	1
Moderate	0	0	1	1

Finally, the scans were performed after installing the all required patches on the machine. There was only one false positive reported by Retina scanner; i.e., the rest of the scanners did not report any.

6 Conclusions

Vulnerability assessment is an important mechanism to provide assurance of appropriate level of confidentiality, integrity and availability of information. It could be used in identifying potential security exposures. Vulnerability scanners are the handy tools used to discover system vulnerabilities in the assessment process. This paper describes a comparative study to find out to what extent a vulnerability scanner can be used to secure a network. This paper compares between four of the leading vulnerability scanners in the market to find out to what extent a vulnerability scanner could be used to secure a network; to find out the scanners effectiveness in detecting Microsoft windows missed patches.

The analysis of the scanners results shows that scanners do not only report unneeded system patches, but also they miss a number of severe patches. After installing the service pack some scanners detection was improved. One of the main challenges for the vulnerability scanners is updating their database with the newly released patches and the replacement for old ones. The analysis of the scanners output shows that not all scanners take into accounts the replaced patches. Moreover, some scanners misreporting some of the replaced patches, consequently increasing the number of false detection.

The findings in this paper points out that system administrators should not depend only on the vulnerability scanners to check for system missed patches, or in tuning other security controls like intrusion detection systems.

References

1. Microsoft Corporation: Microsoft Security Update Guide. 2nd edn. (June 2011)
2. Nist, Aroms, E.: NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment. CreateSpace, Paramount, CA (2012)
3. Danforth, M.: Scalable patch management using evolutionary analysis of attack graphs. In: Proceedings of the 2008 Seventh International Conference on Machine Learning and Applications, ICMLA 2008, pp. 300–307. IEEE Computer Society, Washington, DC (2008)
4. Souppaya, M., Scarfone, K.: Guide to enterprise patch management technologies. National Institute of Standards and Technology, NIST SP 800-40 (September 2012)
5. Yang, G., Chen, D., Xu, J., Zhu, Z.: Research of intrusion detection system based on vulnerability scanner. In: 2010 2nd International Conference on Advanced Computer Control, ICACC, pp. 173–176 (2010)
6. Kavanagh, K.: Marketscope for vulnerability assessment. Gartner, Inc. (August 2011) G00230435
7. Kavanagh, K., Nicolett, M.: Marketscope for vulnerability assessment. Gartner, Inc. (April 2011) G00211846
8. Nilsson, J., Virta, V.: Vulnerability scanners. Royal Institute of Technology, Stockholm (2006)
9. Wack, J., Tracy, M., Souppaya, M.: Guideline on network security testing. National Institute of Standards and Technology, NIST SP 800-42 (October 2003)
10. Beale, J., Deraison, R., Meer, H., Temmingh, R., Walt, C.V.D.: Nessus Network Auditing. Syngress Publishing (2004)
11. Microsoft: Microsoft baseline security analyzer v2.2 (July 2010), `http://microsoft.com/en-us/download/details.aspx?id=7558`
12. McAfee: Mcafee vulnerability manager v7.5 (December 2012), `http://www.mcafee.com`
13. BeyondTrust: Retina network security scanner v5.18 (2012), `http://beyondtrust.com`
14. Rapid7: Nexpose vulnerability management v5.5.12 (2012), `http://www.rapid7.com`
15. Tenable: Nessus vulnerability scanner v5.0.2 (February 2012), `http://www.tenable.com`