Enfoque UTE, V.6-N.3, Sep.2015, pp. 36 - 51
http://ingenieria.ute.edu.ec/enfoqueute/
e-ISSN: 1390-6542 / p-ISSN: 1390-9663
Recibido (Received): 2015/04/30
Aceptado (Accepted): 2015/09/14

Windows Server 2012 vulnerabilities and security

(*Vulnerabilidades y Seguridad de Windows Server 2012*)

Gabriel R. López[1], Danny S. Guamán[1], Julio C. Caiza[1]

Abstract:
This investigation analyses the history of the vulnerabilities of the base system Windows Server 2012 highlighting the most critic vulnerabilities given every 4 months since its creation until the current date of the research. It was organized by the type of vulnerabilities based on the classification of the NIST. Next, given the official vulnerabilities of the system, the authors show how a critical vulnerability is treated by Microsoft in order to countermeasure the security flaw. Then, the authors present the recommended security approaches for Windows Server 2012, which focus on the baseline software given by Microsoft, update, patch and change management, hardening practices and the application of Active Directory Rights Management Services (AD RMS). AD RMS is considered as an important feature since it is able to protect the system even though it is compromised using access lists at a document level. Finally, the investigation of the state of the art related to the security of Windows Server 2012 shows an analysis of solutions given by third parties vendors, which offer security products to secure the base system objective of this study. The recommended solution given by the authors present the security vendor Symantec with its successful features and also characteristics that the authors considered that may have to be improved in future versions of the security solution.

Keywords: Windows Server 2012, vulnerabilities, CVE, operating systems security,

Resumen:
El presente trabajo de investigación analiza la historia de vulnerabilidades del sistema base Windows Server 2012, resaltando las más críticas por cuatrimestres desde su creación hasta la fecha actual organizado por tipo de vulnerabilidad de acuerdo a la clasificación de la NIST. A continuación dadas las vulnerabilidades oficiales, los autores presentan cómo una vulnerabilidad considerada crítica es tratada por Microsoft para mitigarla. Luego los autores proponen medidas de seguridad para Windows Server 2012, donde se enfocan básicamente en baseline de Microsoft, administración de actualizaciones, buenas prácticas de hardening y aplicación de Active Directory Rights Management Services (AD RMS). AD RMS se considera como una valiosa característica que tiene como objetivo la protección del sistema a pesar que éste se encuentre comprometido usando listas de acceso a nivel de documento. Finalmente la investigación del estado del arte de la seguridad de Windows Server 2012 muestra un análisis de soluciones desarrollados por terceros para la protección del sistema operativo objeto del estudio. Como solución de seguridad recomendada los autores presentan a Symantec mostrando sus propiedades de éxito, así como características que podrían ser implementadas en versiones futuras como una oportunidad de mejora.

Palabras clave: Windows Server 2012, vulnerabilidades, CVE, seguridad de sistemas operativos,

[1] Escuela Politécnica Nacional, Quito – Ecuador ({gabriel.lopez, danny.guaman, julio.caiza} @epn.edu.ec)

1. Introduction

Something new in a perfect world maybe perfect, but since IT administrators live in a real world, all pieces of software have problems and errors. The problems that base systems or operating systems may have are known as vulnerabilities. The operating system of a server has vulnerabilities, which are really critical if they are exploited since servers provide services and a disruption may affect a lot of users. This is why the authors have chosen to study the vulnerabilities of Windows Server 2012, which is the last version of the operating systems for Microsoft servers. The study has as its objective to research about the state of the art of the vulnerabilities and security related to Windows Server 2012 since its creation. The investigation starts presenting the current status of its vulnerabilities, which affects the operating system based on the classification used by the National Institute of Standards and Technology (NIST). Each type of vulnerability will be detailed in order from the most common to the less common highlighting the most critical vulnerability of each different kind. In addition, it is showed how one of the most critical vulnerabilities work and how it has been solved by the vendor. Furthermore, the authors suggest Security approaches to mitigate vulnerabilities and security flaws that affect Windows Server 2012. Finally, it is showed how third parties help to protect Windows Server 2012 using as a reference the information technology research and advisory company Gartner.

2. Windows Server 2012 vulnerabilities Review

Windows Server 2012 has experienced 168 official Common Vulnerabilities and Exposures (CVE), according to the database of the National Institute of Standards and Technology (NIST 2015) since its release on September 4th of 2012 (Microsoft 2012) until April 2015 when the investigation was performed. The 168 vulnerabilities of Windows Server 2012 in this period of almost three years has gotten different types of Common Weakness Enumeration (CWE), which helps to categorize the vulnerabilities (CWE 2013). To begin, the majority of CWE for Windows Server 2012 are Permissions, Privileges and Access Control with the 25% of the total (See *Table 1*), which means that the system has problems in managing access restrictions. *Table 1* shows the Common Weakness Enumeration (CWE) of Windows Server 2012, which is a list of software weaknesses about the operating system; with the corresponding numbers of vulnerabilities found in a period of every 4 months since the release of the software. The vulnerabilities of this CWE cause in general gain privileges attacks, man in the middle attacks and remote or physically code execution with a USB, which could provoke a denial of service. The vulnerabilities CVE-2013-3175 published on August 14th of 2013 and CVE-2013-0073 published on February 13th of 2013 have both a CVSS (Common Vulnerability Scoring System) of 10.0, so they are the most dangerous of the CWE of Permissions, Privileges and Access Control. These vulnerabilities allows the attacker to do a remote code execution (NIST 2015).

Table 1. Vulnerabilities of Windows Server 2012 classify by CWE (NIST 2015).

	2012	2013			2014			2015	2012 - 2015	
CWE	**September - December**	**January - April**	**May - August**	**September - December**	**January - April**	**May - August**	**September - December**	**January - April**	**#**	**%**
Permissions, Privilegies and Access Control	1	6	4	2	3	7	4	15	42	25
Buffer Errors	1	3	7	8	3	2	0	2	26	15
Resource Management Errors	2	12	1	2	1	2	1	2	23	14
Code Injection	1	1	2	2	0	1	5	8	20	12
Input Validation	2	2	0	6	1	4	2	2	19	11
Information Leak / Disclosure	0	1	1	1	0	0	1	8	12	7
Other	1	1	1	0	0	1	1	6	11	7
Numeric Errors	2	1	0	2	0	0	0	0	5	3
Race Conditions	0	4	0	0	0	0	0	0	4	2
Insufficient Information	0	2	0	0	0	1	0	1	4	2
Path Traversal	0	0	1	0	0	0	0	1	2	1
Total	**10**	**33**	**17**	**23**	**8**	**18**	**14**	**45**	**168**	**100**

The second most popular type of CWE for Windows Server 2012 are Buffer Errors with a 15% of the total of vulnerabilities (See *Table 1*). This security issue in general helps the hacker to gain access and do a remote code execution. The vulnerability CVE-2012-2897 published on September 26th of 2012 has the highest Common Vulnerability Scoring System (CVSS) of 10.0 in the Buffer Errors CWE. In this vulnerability, the kernel-mode drivers do not manage correctly the objects in memory, causing that the attacker can do a remote code execution (NIST 2015).

The third most popular type of CWE for Windows Server 2012 is the resource management errors with 14% of the total (See *Table 1*), which means that the hackers exploits the lack of control in manipulating disk, memory or CPU of the server. This type of flaw provokes in general the vulnerability of remote code execution. The vulnerability with the highest CVSS in the Resource Management Errors CWE is CVE-2013-3195, which was published on October 9th of 2013 and it has a CVSS of 10.0. The security issue for this case is that the DSA_InsertItem function in Comctl32.dll is not assigning memory correctly, so it causes the problem of remote code execution (NIST 2015).

The CWE of code injection represents the 12% of the vulnerabilities for Windows Server 2012 (See *Table 1*). This flaw is related directly to vulnerabilities that allows the hacker to perform remote code execution. In general this types of vulnerabilities have the highest Common Vulnerability Scoring System (CVSS) (NIST 2015) because the hacker could be able to get full control over the server. Five vulnerabilities that are part of the Code Injection CWE have the highest CVSS of 9.3. CVE-2013-3894 published on October 9th of 2013, CVE-2013-3174 published on July 7th of 2013, CVE-2013-3129 published on July 10th of 2013, CVE-2013-0007 published on January 9th of 2013 and CVE-2012-2556 published on December 12th of 2012 have the security issue of allowing the attacker to do a remote code execution (NIST 2015) as it is shown in *Table 2.*

Table 2. Critical vulnerabilities for the CWE of code injection.

CVE	Published Date	CWE	CVSS
CVE-2013-3894	09/10/2013	Code Injection	9.3
CVE-2013-3174	07/07/2013		
CVE-2013-3129	10/07/2013		
CVE-2013-0007	09/01/2013		
CVE-2012-2556	12/12/2012		

The 11% of the Windows Server 2012 vulnerabilities are about input validation problems (See *Table 1*), which in other words means that some data is not being checked to be valid. This kind of CWE is related with vulnerabilities which in general could cause denial of service, malicious remote code execution or man in the middle attacks. The vulnerabilities with the highest CVSS of 9.3 are

CVE-2013-3128 published on October 10th of 2013, CVE-2013-0004 published on January 9th of 2013 and CVE-2012-4776 published on November 14th of 2012. The three vulnerabilities permit the attacker to do a remote code execution (NIST 2015).

The CWE for information leak/disclosure and other represents the 7% of the vulnerabilities of Windows Server 2012 (See *Table 1*). This CWE means that the system has problems exposing private information, which could lead to have vulnerabilities that will allow to obtain sensitive information of the system. The vulnerability CVE-2013-3185 published on August 14th of 2013 has the highest CVSS of 5.0 in the Information Leak / Disclosure CWE. In this vulnerability, Active Directory Federation Services permits the attacker to get private information of the service account (NIST 2015).

The numeric errors CWE represents the 3% of the vulnerabilities of Windows Server 2012 (See *Table 1*), this flaw happens when the system gets errors when handling numbers. The vulnerabilities related to this CWE may be able to cause attacks like gain privileges, remote code execution or denial of service. Four vulnerabilities that are part of the Numeric Errors CWE have the highest CVSS of 9.3. CVE-2013-3940 published on November 13th of 2013 and CVE-2013-0006 published on January 9th of 2013 have the security issue of allowing the attacker to do a remote code execution. CVE-2012-1528 published on November 14th of 2012 and CVE-2012-1527 published on November 14th of 2012 have the security issue of allowing the attacker to gain privileges (NIST 2015).

The CWE of race conditions is just the 2% of vulnerabilities of Windows Server 2012 (See *Table 1*) and it represents problems about instability of the state of a resource. The CWE of this type in general generates vulnerabilities that allows to gain privileges. Two vulnerabilities that are part of the Race Conditions CWE have the highest CVSS of 6.9. CVE-2013-1292 and CVE-2013-1283 both published on April 9th of 2013 have the security issue of allowing the attacker to gain privileges (NIST 2015).

The 2% of the vulnerabilities of Windows Server 2012 are considered that do not have a category of CWE or there is not sufficient information to classify them (See *Table 1*). In the category of insufficient information to classify the vulnerability as part of a CWE, the one with the highest CVSS of 9.3 is CVE-2013-0074 published on November 3rd of 2013. This vulnerability allows the attacker to do a remote code execution (NIST 2015).

Finally, the path traversal CWE is only the 1% of the vulnerabilities of Windows Server 2012 (See *Table 1*). The vulnerability related to this CWE provokes a denial of service. The only vulnerability of this category of CWE is the CVE-2013-3661 published on May 24th of 2013. In this vulnerability, the EPATHOBJ::bFlatten function in win32k.sys allows the attacker to perform a denial of service (NIST 2015).

The figure 1 shows the official vulnerabilities of Windows Server 2012 from September 2012 to April 2015 classified by the type of CWE based on the NIST classification.

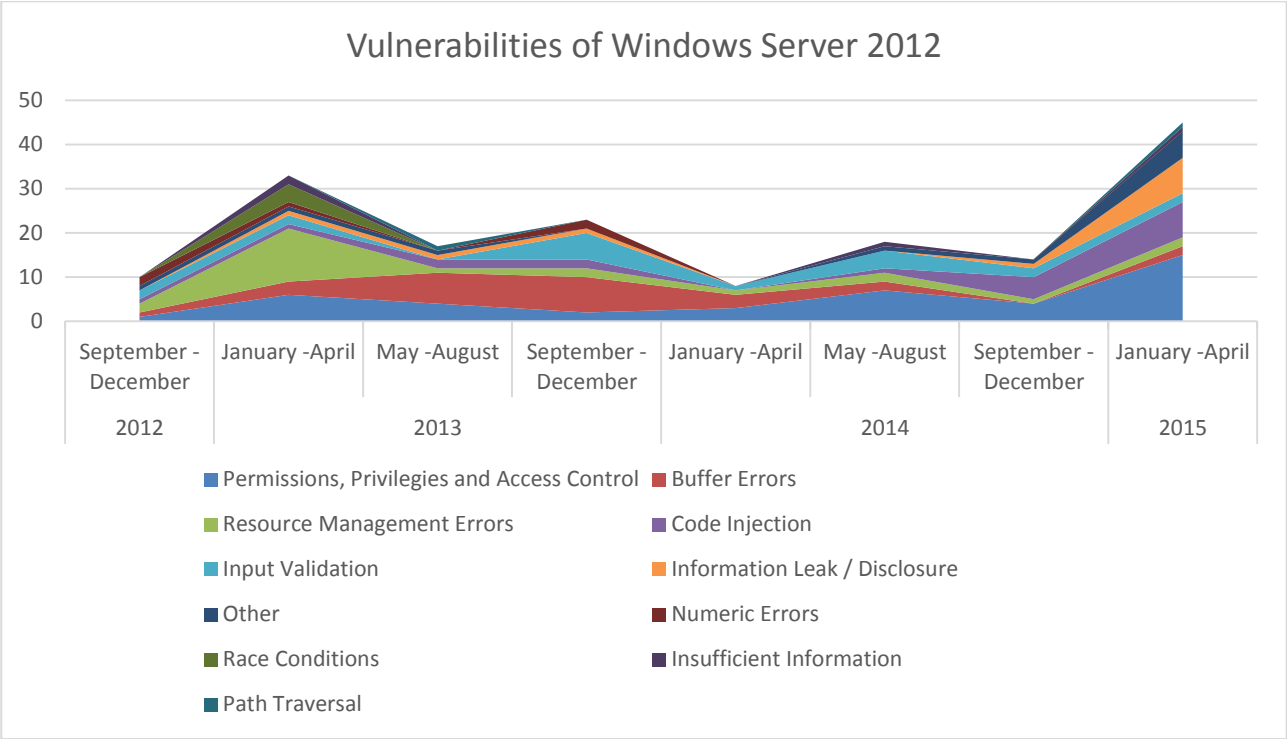

Figure 1. Vulnerabilities of Windows Server 2012

Figure 1 shows that Windows Server 2012 from September 2012 to the period of May-August 2013 the vulnerability related to Resource Management Errors has the dominance in comparison with the other vulnerabilities, but since that period of time the CWE that starts to grow is Buffer Errors until January-April 2014. Finally the vulnerability type that has more official CVE related is Permissions, Privileges and Access Control, which started to increase in the period of January-April 2014 and kept the dominance until the current period of January-April 2015.

3. Solution for a critical vulnerability of Windows Server 2012

Firstly, the authors have chosen the vulnerability CVE-2013-3195 due to its high CVSS, recentness and type of CWE. To begin, the vulnerability due to the impact of 10.0, which means that it has a complete impact on the metrics of confidentiality, integrity and availability. The exploitability has also a value of 10.0 because its access vector is the network, the access complexity is low and it does not require authentication (NIST 2015), so an attacker will be able to access remotely and without a high complexity. In addition, the CVE-2013-3195 is the last official CVE vulnerability published on December 20th of 2013, which has the max CVSS of 10.0 for Windows Server 2012. Finally the type of CWE for CVE-2013-3195 is resource management errors, which is critical for servers. This type of vulnerability could provoke that an external agent may take control of the resources of a company, so the investment in the case of a server asset will not generate a benefit for the organization if the server is compromised.

Secondly, the CVE-2013-3195 generates a problem which allows the hacker to execute arbitrary code. The root cause of the security issue is that the DSA_InsertItem function in Comctl32.dll, has problems allocating memory, so the attacker via network can do an execution of a malicious code (NIST 2015). The function specifically puts a new item inside the dynamic structure array (DSA) (Microsoft 2015). Moreover, the hacker in order to perform the attack can use a shaped value in an argument placed to an ASP.NET web application, so this vulnerability is very critical for web application servers. If the attacker can exploit this vulnerability can get the same privileges of logged on user or a local user (NIST 2015). Also, this vulnerability only applies for systems of 64-bit, since for 32-bit architectures this kind of attack vector is block by default in its configuration (Microsoft 2015). Finally, exploits have not been developed for this vulnerability (Offensive Security 2015).

Thirdly, Microsoft has developed updates in order to countermeasure the vulnerability CVE-2013-3195. The solution has been published in the Microsoft Security Bulletin MS13-083 (US-CERT 2014), where the vulnerability has been identify as Vulnerability in Windows Common Control Library with the ID 2864058 (Microsoft 2015). The security update has been classified as critical for all 64-bit MS operating systems and it fixes the vulnerability because it correct the procedure that the Windows common control library assigns memory for data structures. The Security Update for Windows Server 2012 (KB2864058) can be downloaded from the Download Center of Microsoft by the file name Windows8-RT-KB2864058-x64.msu (Microsoft 2015). After the installation of the update, the system has to be restarted. In addition, the recommendations to prevent to have problems with this kind of vulnerability are: deny external access to the server unless is necessary, run software with users which have only the minimum and required privileges, the use of memory-protection schemes, like non-executable stack/heap configurations (Symantec Corporation 2015).

It is important to mention that all the vulnerabilities presented in this section have been patched by a Microsoft update since they do not represent zero-day attacks. Generally speaking, the vulnerabilities formally presented by CVE, NIST and Microsoft have its solution published in the Microsoft security Bulletin, which is realised on the Second Tuesday of each month (Microsoft 2015).

4. Security approaches for Windows Server 2012

Firstly, Microsoft Windows recommend the use of the tool Windows Server 2012 Security Baseline in order to configure general best security practices for this operating system. To begin, this tool helps to plan, deploy and monitor security hardening for the system (Microsoft 2015). The Baseline software is a compendium of procedures for secure configuration of Windows Server 2012, which shows the administrator a list of vulnerabilities related to the install environment of Windows Server 2012 in order to recognize threats, as well as recommendations supported with technical information in order to apply countermeasures to solve the security issues. The security baseline is

managed by the Microsoft Security Compliance Manager tool (SCM tool), which provides a centralized point of administration for viewing, exporting and updating security baselines (Microsoft 2015). Also, Windows Server 2012 Security Baseline is provided for both versions: Windows Server 2012 and Windows Server 2012 R2 (Microsoft 2015). In addition, Microsoft provides the Microsoft Security Assessment Tool 4.0, which measures the security approaches related to people, process and technology. It is composed of various questions related to best practices like ISO 17799 and NIST-800.x, as well as from the Microsoft's Trustworthy Computing Group. After finishing the assessment a report will be given with the results (Microsoft 2015). Moreover, the administrator of a Microsoft Windows Server 2012 platform should consider the built-in technology of the system to improve its security in the areas of authentication and identity, authorization and isolation, data protection and secure networking. In a following part of this essay, it will be discussed the important tool Active Directory Rights Management Services, which helps to preserve authentication and identity, authorization and isolation and data protection (Microsoft 2015).

Secondly, it is recommended to consider the security approaches of Windows Server 2012 for patch management, security auditing and various new features of the system. To begin, patch management is necessary for every organization. Since software is developed by humans, it has errors in its code, consequently the programs have vulnerabilities that can be exploited by hackers (zero-day attacks) or in the best case can be found by researchers. This is why Microsoft releases every period of time new security updates in order to countermeasure flaws of the system. In the case of the server it is recommended to activate the Windows Server Update Services, but every update must be first planned in order to mitigate the risk of a vulnerability. An administrator should know that testing the update is crucial to make sure that it will not generate an incompatibility in the production system. According to Shinder, Diogenes and Shinder (2013) the phases to deploy security updates are: planning, availability for download, obtain the files, create update, test and deploy in production. In addition, the auditing logs are necessary for the administrators to basically monitoring activities and forensic analysis (Microsoft 2015). It is recommended to activate the security auditing for critical information assets of the company. Finally the authors recommend to review new security features of Windows Server 2012, such as Active Directory Federation Services (ADFS), principle of isolation in virtualization, Dynamic Access Control (DAC), SMB 3 encryption, Windows Firewall with Advanced Security, Microsoft Security Essentials, IPsec, port ACLs, bandwidth control, DHCP protection, router advertisement protection and good practices for cloud security.

Thirdly, the authors presents the technology of Active Directory Right Management Services. To begin, information is the most important asset of an organization and it is in general the most important objective of a hacker. Windows Server 2012 provides an enhanced feature to protect information disclosure called Active Directory Right Management Services (AD RMS). Moreover,

the administrator can perform all the best practices and system hardening, but the system could still suffer an attack. Enabling AD RMS in Windows Server 2012 will help to prevent information disclosure, even if the network, operating system and application have been compromised. (Shinder, Diogenes and Shinder 2013). Furthermore, AD RMS applies a high level of access control list to the document. WikiLeaks is an example of how private information of a company can end in the wrong hands. In general the majority of information for WikiLeaks was accessed by personal with not high privileges. This vulnerability in general takes place when the administrator works with permissions in nested groups, which leads to misunderstanding with the real permissions that are being established, so a better way to make sure that a user should be granted to information access is the AD RMS. The AD RMS assigns permissions at a document level instead in the file level, so when an administrator sets restrictions at the document level, all the shared permissions at a file level will not be considered. Also the document can be forbidden to be read out of the domain and the permissions can be granular, such as just read, but not copy or modify. In addition, this feature can be applied in the cloud and will check access in Office, Exchange and SharePoint (Shinder, Diogenes and Shinder 2013). Since AD RMS works in cooperation with exchange, it can check if a user is allowed to send sensitive information, so if it is permitted, when someone receives the message, the receptor can only open the document if first it is available an AD RMS to approve it, then it will be allowed or denied. Consequently, if an internal attacker finds the way to copy critical information of the organization to an external storage, he will not be able to open it if he does not have the permission (Thomas 2010). In addition, the deployment of AD RMS needs some general considerations. First it is needed one AD RMS per forest in the Active Directory network and also it is recommended to have a cluster of this servers to assure availability of the service. Also, the server should have a hardware dedicated only to AD RMS, this is to prevent the mix of server roles. (Shinder, Diogenes and Shinder 2013).

5. Third Party, protection for Windows Server 2012

Firstly, the authors analysed that a suitable protection mechanism for Windows Server 2012 is an Endpoint Protection Platform. To begin, the leaders in the market according to Gartner (2014) in the Magic Quadrant for Endpoint Protection Platforms are McAfee, Kaspersky, Symantec, Trend Micro and Sophos because of its completeness of vision and the ability to execute as it is shown in *Figure 2*. McAfee and Kaspersky give a good approach to Endpoint Security but they do not have a product directly oriented to server security. They provide a software solution for business or enterprises in general (McAfee 2015; Kaspersky 2015). On the other hand, Symantec, Trend Micro and Sophos provide a solution to secure servers, but each one has a different approach to secure the IT environment. Trend Micro is very strong in the field of cloud and virtualization security with its product Cloud and data center security (Trend Micro 2015). Sophos with its product Server Protection is adequate for malware and virtual environments, but it is not cloud security oriented (Sophos 2015). Symantec with its product Critical System Protection provides a holistic analysis

including protection to virtual systems, cloud, HIPS/HIDS and Active Directory integration (Symantec 2015). Moreover, in the report of Gartner 2013 on March 27th of 2013 Symantec got the best position in the Magic Quadrant for Endpoint Protection Platforms (Gartner 2013) and for the report on January 8th of 2014 Symantec maintains as one of the leaders in the Magic Quadrant for Endpoint Protection Platforms. Consequently, the authors has chosen Symantec for its analysis because of the advantages that the product provides.

Figure 2. Leaders in the Gartner Magic Quadrant for Endpoint Protection Platforms (Gartner 2014).

Secondly, the Symantec Critical System Protection is a server oriented solution. To begin, Symantec will allow to maintain a centralized security policy administration since the solution integrates with the Active Directory of Windows Server 2012 (Symantec 2015). In addition, Symantec provides technology for security prevention. The first point of security will be the HIDS/HIPS included in the solution. Also, it is provided a memory control to prevent attacks, which will protect from possible vulnerabilities of the system. A host firewall is also included to control network connections to the server. Finally, a technology called Process Access Control provides control over running process, which will allow to do an in deep intrusion prevention action (Symantec 2015). In addition, Symantec offers features to perform countermeasures under attacks. In the case of an attack, it provides prevention policies, which will use premade functions and will work in coordination with the HIDS and HIPS policies. Also, it is provided a lock down configuration in order to preserve the server's security in terms of confidentiality, integrity and availability.

Thirdly, Symantec solution protects virtual environments, manage patching and support security compliances. To begin, the solution provides good practices for vSphere hardening, which is the main administration structure of a virtual system using VMware. Consequently, it provides security

at the levels of server management (VMware vCenter™ management server protection), hypervisor (VMware ESX® and VMware ESXi™ hypervisor protection), which runs the virtual servers and guests (VMware ESX and ESXi guest protection) (Symantec 2015). In addition, patching helps to countermeasure the vulnerabilities of the systems. If the software does not have support anymore it will be a challenge for the IT administrator to protect it and if the applications do have support, the system will be vulnerable during the time needed by the vendor to generate the patch. Symantec gives a solution for these cases providing system hardening, locking of the configuration, and restrictions of system's behaviour. Finally, Symantec helps to check the state of a policy compliance, such as PCI. It monitors in real time the server activity in order to verify, collect logs and prevent policy violations (Symantec 2015).

Finally, even though Symantec is a leader in Endpoint Security Platforms, it presents some opportunities for improvements (Gartner 2014). To begin, Symantec may improve in developing new features like forensic discovering capabilities for better understanding of what happened after an attack and implementing a network-based sandbox to analyse suspicious code and report. In addition, Symantec may improve in current capabilities such us weak proactive security assessment. This in order to inform to the IT security professional ahead of time of possible problems that the system may have. Also, the Control Compliance Suite is not part of the main console of Critical System Protection. This makes it difficult for the administrator because he has to consolidate information from both consoles. Finally, the set of policies for encryption in removable devices is not easy to understand. It is preferred that the IT administrator has a tool which provides an easy and clear configuration in order to secure the systems on the fly and correctly. *Table 3* shows a summary of the characteristics of the Symantec security solution for Windows Server 2012.

6. Further research

The further research work suggested by the authors recommends to use automatic tools of pen testing in order to confirm that after all the hardening and security of the base system Windows Server 2012, the vulnerabilities does not exist anymore or are mitigated.

7. Conclusions

The most common vulnerability or Common Weakness Enumeration (CWE) for Windows Server 2012 is the Permissions, Privileges and Access Control represented by the 25% of the total of vulnerabilities officially recognized and each year it has been increasing its number of vulnerabilities related. The vulnerability is dangerous since it exploits the bad management of access restrictions of the operating system, which will provoke a privilege escalation and enable the attacker to execute malicious code on the victim.

Table 3. Symantec Critical System Protection (Symantec 2015).

	Characteristics	**Description**
Security Features	Virtual Systems	Protects virtual environments: - System hardening - Locking of the configuration - Restrictions of system's behaviour
	Cloud	Cloud security oriented
	HIPS/HIDS	Security prevention: - Memory control to prevent attacks - Host firewall - Process Access Control - Premade functions - Lock down configuration
	Active Directory integration	Capable of using Active Directory configuration policies.
Opportunities for improvements	Forensic discovering capabilities.	
	Weak proactive security assessment.	
	Consolidate consoles of the solution.	
	Unfriendly policies for encryption in removable devices.	

The second most common vulnerability for Windows Server 2012 are the Buffer Errors type. This CWE as the Permissions, Privileges and Access Control let the hacker to gain access to perform a remote code execution, but the difference is that Buffer Errors have the flaw of not managing correctly objects in memory provoking the attacker to execute his code.

The third most common vulnerability is resource management errors, which the same as Common Weakness Enumeration and Buffer Errors enables the attacker to perform a remote code execution, but this vulnerability exploits the lack of control in manipulating disk, memory or CPU of the server.

The forth most common vulnerability is code injection, which is one of the most dangerous since it let the attacker to execute directly malicious code. The first three most common vulnerabilities exploit different flaws looking for a remote code execution.

The fifth most common vulnerability is related to input validation problems, which exploits data that is not being checked or sanitized. This vulnerability as the other four enable the attacker to execute malicious code also denial of service and man in the middle attacks.

The sixth most common vulnerability is leak disclosure, which enables the attacker to obtain sensitive information of the system. This vulnerability does not focus on the remote code execution of malicious code.

The seventh most common vulnerability is the CWE numeric errors, which allows to perform a remote code execution like the first five most common vulnerabilities, gain privileges and denial of service. This vulnerability is exploited by the attacker when the system gets errors when handling numbers.

The eight most common vulnerability presents instability problems of the state of a resource and enables gain privileges to the attacker.

The ninth most common vulnerability is the CWE that does not have a specific classification because its vulnerabilities does not provide enough information to be part of a CWE group. This vulnerability cannot be classified to have a certain type of attack vectors.

The tenth most common vulnerability is the path traversal which provokes denial of service to the applications running over Windows Server 2012.

8. Recommendations

The security vulnerabilities can be counter measured by applying the updates released by Microsoft, but it is recommended to use a change management policy. It is not a good practice to have automatic updates in the server since they may produce an incompatibility with other software of the system. Also users are suggested to have only the privileges that they require and memory-protection schemes, like non-executable stack/heap configurations.

The security approaches recommended by the authors suggest to implement security baseline from Microsoft to check the system based on good security practices, such as ISO 17799 and NIST-800.x. Also, it is recommended to implement the enhanced feature of Microsoft Windows Server 2012 to protect information disclosure called Active Directory Right Management Services (AD RMS). This feature will protect the most important asset of the company, which is the information. It will protect the system even though the base system is compromised since AD RMS applies a high level of access control list to the document.

The third party protection solution for Windows Server 2012 recommended by the authors is Symantec with its product Critical System Protection due to holistic analysis including protection to virtual systems, cloud, HIPS/HIDS and Active Directory integration. This vendor offers a server oriented solution, which work in a proactive way having countermeasures under attack and lock down configuration in order to preserve the confidentiality, integrity and availability. Also, Symantec offers a hardening feature for virtual systems using VMware and in the scenario that a system is not supported anymore, such as Windows Xp, Symantec provides a solution to restrict the

behaviour of the system in case of a known vulnerability. Finally, the authors highlight that the Symantec solution even though is the recommended third party vendor, it has to improve in the following aspects: forensic discovering capabilities, network-based sandbox, proactive security assessment, consolidate consoles of the solution.

References:

CVE (2015). CVE List Master Copy. [online]. Last accessed 16 March 2015 at: http://cve.mitre.org/cve/cve.html

CWE (2015). CWE List. [online]. Last accessed 16 March 2015 at: http://cwe.mitre.org/data/index.html

GARTNER (2013). Magic Quadrant for Endpoint Protection Platforms. [online]. Last accessed 21 March 2015 at: http://www.gartner.com/technology/reprints.do?id=1-1DFHJZW&ct=130102&st=sb

GARTNER (2014). Magic Quadrant for Endpoint Protection Platforms. [online]. Last accessed 21 March 2015 at: http://www.gartner.com/technology/reprints.do?id=1-1P53WTD&ct=140108&st=sb

KASPERSKY (2015). Endpoint Security for Business Core. [online]. Last accessed 21 March 2015 at: http://www.kaspersky.co.uk/business-security/endpoint-core#tab=frame-2

MCAFEE (2015). McAfee Complete Endpoint Protection — Enterprise. [online]. Last accessed 21 March 2015 at: http://www.mcafee.com/us/products/complete-endpoint-protection-enterprise.aspx#vt=vtab-Benefits

MICROSOFT (2015). Microsoft Security Bulletin. [online]. Last accessed 27 July 2015 at: https://technet.microsoft.com/en-us/security/bulletin/dn602597.aspx

MICROSOFT (2015). Windows Server Blog. [online]. Last accessed 15 March 2015 at: http://blogs.technet.com/b/windowsserver/archive/2012/08/01/windows-server-2012-released-to-manufacturing.aspx

MICROSOFT (2015). Windows Develop Center – Desktop. [online]. Last accessed 16 March 2015 at: http://msdn.microsoft.com/en-us/library/windows/desktop/bb775665(v=vs.85).aspx

MICROSOFT (2015). Security TechCenter. [online]. Last accessed 16 March 2015 at: http://technet.microsoft.com/en-us/security/bulletin/ms13-083

MICROSOFT (2015). Download Center. [online]. Last accessed 16 March 2015 at: http://www.microsoft.com/en-us/download/details.aspx?id=40408

MICROSOFT (2015). Windows Server 2012 Security Baseline. [online]. Last accessed 17 March 2015 at: http://technet.microsoft.com/en-us/library/jj898542.aspx

MICROSOFT (2015). Microsoft Security Assessment Tool 4.0. [online]. Last accessed 17 March 2015 at: http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=12273

MICROSOFT (2015). Secure Windows Server 2012 R2 and Windows Server 2012. [online]. Last accessed 17 March 2015 at: http://technet.microsoft.com/en-us/library/hh831360.aspx

MICROSOFT (2015). Security Auditing Overview. [online]. Last accessed 17 March 2015 at: http://technet.microsoft.com/en-us/library/dn319078.aspx

NIST (2015). National Vulnerability Database. [online]. Last accessed 16 April 2015 at: http://web.nvd.nist.gov/view/vuln/search-advanced

OFFENSIVE SECURITY (2015). Exploit Database. [online]. Last accessed 16 March 2015 at: http://www.exploit-db.com/search/

OPEN VULNERABILITY AND ASSESSMENT LANGUAGE. (2015). Oval Repository. [online]. Last accessed 16 March 2015 at: http://oval.mitre.org/repository/

SHINDER, Thomas W., DIOGENES, Yuri and SHINDER, Debra Littlejohn (2013). Windows server 2012 security from end to edge and beyond: Architecting, designing, planning, and deploying windows server 2012 security solutions. [online]. Elsevier. at: http://shu.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwY2AwNtIz0EUrE9KMLJIskyySjM0Tk02SDQ0SLUySQKdppSVbWpqkgC9VQBxjgFTAuwkxMKXmiTLIuLmGOHvoFmeUxkOHNeKTgG1pYG0FrPHFGFiAXeVUAPLTHTc.

SOPHOS (2015). Server Protection. [online]. Last accessed 21 March 2015 at: http://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-server-protection-dsna.pdf

SYMANTEC (2015). Symantec Critical System Protection. [online]. Last accessed 21 March 2015 at: http://www.symantec.com/critical-system-protection

SYMANTEC (2015). Data Sheet: Endpoint Security. [online]. Last accessed 21 March 2015 at:http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-critical_system_protection_ds_21197836-3_1212.en-us.pdf

SYMANTEC CORPORATION (2015). Security Response. [online]. Last accessed 21 March 2015 at: http://www.symantec.com/security_response/vulnerability.jsp?bid=62801

THOMAS, Orin. (2010). How AD-RMS can stop your organization's secrets ending up on Wikileaks. [online]. Last accessed 16 March 2015 at: http://windowsitpro.com/blog/how-ad-rms-can-stop-your-organization-s-secrets-ending-wikileaks

TREND MICRO (2015). Cloud and data center security. [online]. Last accessed 21 March 2015 at: http://www.trendmicro.co.uk/enterprise/cloud-data-center-security/

US-CERT (2015). Microsoft Updates for Multiple Vulnerabilities. [online]. Last accessed 16 March 2015 at: http://www.us-cert.gov/ncas/alerts/TA13-288A