Часопис из области економије
менаџмента и информатике
Година 2018, волумен 9, број 1, стр. 19-29

Journal of Economics, Management
and Informatics
Year 2018, Volume 9, Number 1, pp. 19-29

Прегледни рад/ Reviewing paper

УДК/UDC: 004.383.2:004.738.1]:004.056.5

IMPORTANCE OF VULNERABILITY SCANNERS FOR IMPROVING SECURITY AND PROTECTION OF THE WEB SERVERS

ЗНАЧАЈ СКЕНЕРА РАЊИВОСТИ ЗА УНАПРЕЂЕЊЕ БЕЗБЕДНОСТИ И ЗАШТИТЕ ВЕБ СЕРВЕРА

Darjan Karabašević[1]
Faculty of Applied Management, Economics and Finance, University Business Academy in Novi Sad

Dragiša Stanujkić
Technical faculty in Bor, University of Belgrade

Miodrag Brzaković
Faculty of Applied Management, Economics and Finance, University Business Academy in Novi Sad

Mlađan Maksimović
Faculty of Applied Management, Economics and Finance, University Business Academy in Novi Sad

Milena Jevtić
Technical faculty in Bor, University of Belgrade

Abstract: *Technological development, in particular information and communication technologies (ICT), has caused the most immediate and quickest changes in the everyday way of life of people. The result of this is the world we have today, all around us are computers that are an integral part of our everyday life, while at the same time we use the networks constantly and everywhere. The Internet (the network of all networks) is the media we rely*

[1] darjankarabasevic@gmail.com

on in our work, gives us answers to all questions, concerns and topics that interest us, helps us learn and transfer data for any purpose. But, Internet often can be an insecure place and that it represents a connection of all those who want to be involved, including those malicious. A very important and very complex step in securing networks and network systems is the vulnerability assessment. Therefore, the paper aims to point out the importance of the vulnerability scanners in improving the security and protection of the web servers.
Key words: *Vulnerability Scanners, Web Servers, Protection and Security, Vulnerability Assessment*

Сажетак: *Технолошки развој, посебно информационо-комуникационих технологија (ИКТ) изазвао је најкоренитије и најбрже промене у свакодневном начину живота људи. Резултат тога је свет какав данас имамо, свуда око нас су рачунари који представљају саставни део наше свакодневнице, док истовремено мреже непрестано и свугде користимо. Интернет (мрежа свих мрежа) је медији на који се ослањамо у послу, даје нам одговоре на сва питања, недоумице и теме које нас занимају, помаже нам у учењу и преносу података у било коју сврху. Али, Интернет често уме да буде и несигурно место и да представља спој свих оних који желе да буду укључени, обухватајући и оне злонамерне. Веома битан и веома сложен корак у осигуравању мрежа и мрежних система јесте процена рањивости. Стога, рад има за циљ да укаже на значај скенера рањивости за унапређење безбедности и заштите веб сервера.*
Кључне речи: *Скенери рањивости, веб сервери, заштита и безбедност, процена рањивости*

1. INTRODUCTION

We live in a era of constant change and development in many areas. This era is constantly under the influence of technology developments, especially in terms of information and network technologies. The growth of data transfer speeds and the development of many Internet-based technologies has led to a new, "smaller" world that depends on information technology and the network (Krštenić, 2016).

Over the past decades, business has changed radically as well as a way of communicating with employees, suppliers and customers. The need for information forced the man to establish relationships with various sources of information and to create networks which will itself facilitate the collection, transmission, storage and processing of data. With the rapid development of computer technology in recent years (increasing performance with falling prices) and with real Internet explosion, the number of computer users and

computer networks has grown at a fast paced speed. With increasingly powerful computer equipment, new services are being introduced on a daily basis, while at the same time higher standards are set in the networking, so today the network systems have reached the level of a practical, efficient data exchange environment, which allowed the development of a new type of business operations.

Web is increasingly being used for different types of services as well as for interacting with, and between humans. Beyond displaying static content such as home pages or academic papers, the web is actively used for various tasks such as e-mails, banking, online shopping, marketing and real-time communications. The widely available high-quality browsers and servers, as well as the programmers' and users' familiarity with the tools and concepts behind web browsing ensure that ongoing creation of additional services. Such an environment provides a rich set of targets for motivated attackers. This has revealed by a large number of vulnerabilities and exploits on web servers, browsers, and applications. Traditional security considerations are about protecting the confidentiality and integrity of the network connection, protecting the server from break-in and protecting client's private information from unintended disclosure. For this purpose, several protocols and mechanisms have been developed, dealing with these issues individually. However, one area that has been neglected for a long time is the availability of the service in the presence of DoS attacks and their distributed variants (DDoS) (Morein et al., 2003).

Security is a common area of concern both for service providers and for users. Therefore, it is a priority that needs to be solved as soon as possible within the IT industry. Failures in the security of software and web servers can be very problematic for information systems, especially those in commercial applications that work with a large amount of confidential data, and this is a topic that is highly represented in modern computing. As the amount of data increases at a high speed and there is an increasing number of applications running on the web, it is expected that the significance of this problem is becoming more and more important (Von Solms & Van Niekerk, 2013).

It can be said that most of today's cyber-attacks are the result of well-known failures and vulnerabilities. The abundant dependence on technology and related services increases the number of devices, databases and software solutions present in everyday business. This affects the constant increase in the number of recognized and "misused" vulnerabilities and omissions (Hug & Giampapa, 2012).

In today's complex environment of malware, spyware, employee dissatisfaction and more and more aggressive hackers, the development and consistent implementation of a good network security policy, including vulnerability scanning, is critical to maintaining continuity and continuity of operations. It can be said that vulnerability assessments and recovery procedures have become critical components of good practices in information security management.

Scanning a computer network is crucial to collect information about the real state of the client / server operating systems, as well as network devices. It is also a way to identify and find active network devices with the ultimate goal of making and assessing security of the boundary. The vulnerability assessment is a systematic analysis of the security state of the information system. Both of these techniques are the most comprehensive for auditing, penetration tests, reporting and installing patches for the information system of any organization.

Based on the above, the paper aims to point out the significance of vulnerability scanners for improving security and protecting the web servers. Therefore, the work is organized as follows. In section 1, introductory considerations are given, section 2 represents the security of the web server and recommendations for improving security, section 3 represents NESSUS - a case study and section 4 presents concluding considerations.

2. SECURITY OF THE WEB SERVERS AND RECOMMENDATIONS FOR IMPROVING SECURITY

We live in the age of technology. It is constantly there in all spheres of our lives. In a private and business life, we cannot use the vast majority of technology products. To make it easier for us to do some things, it has led to many changes in various industries.

In modern times, many hacking attacks make it clear to us how many servers are "vulnerable" and how important their protection is. Protecting the web application itself will not be too useful if our server is unsafe. Items that are important for protecting web servers are: Removing unnecessary services; Remote access; Maintenance of user accounts; Permissions and privileges; Server monitoring; Separating applications and scripts; Separating development and test environments. These measures do not guarantee, but greatly contribute to increasing the security of web servers and it is advisable to adhere to them during its maintenance.

Company Acunetix from its experience and many years of work in the field of web server security and database server security propose recommendations for improving security (Acunetix, 2018):

- ***Removing unnecessary services*** is desirable because every service that is used on the web server opens a new port on it. In this way, the number of weak points of the server increases, and it is more difficult to maintain. Also, by eliminating unnecessary services, we can get an increase in performance with the services used.
- ***Remote access*** is used by web server administrators. Although it is recommended that the maintenance work locally, sometimes it is not possible, and it is necessary to have this option enabled on the web server. It is useful to limit this approach to the server to only specific accounts and IP addresses, in order to reduce the security risk caused by its enabling.
- **Maintaining user accounts**, such as removing unnecessary services, reduces the number of risky sites in the web server. It is desirable to remove or limit privileges of accounts created during the configuration of the operating system or additional applications.
- ***Permissions and privileges*** should be set according to the real needs of the services used. If privileges override the needs, a malicious user can use this for unwanted operations over the information on the server.
- **Server monitoring** involves monitoring reports, both systemic and application-specific. In this way, it is possible to spot the unusual behavior of the applications in a timely manner and prevent possible abuse of defects, but also to notice the attempted attacks.
- ***Separating applications and scripts*** from the operating system and other system data is highly desirable. Namely, hackers accessing the root directory can often get very high privileges to freely use all the functions of the operating system. This limits the problem of insufficient security of the application so it does not affect other applications stored on that server.
- ***Separation of the development and the public environment*** provides additional security if the development environment is not publicly available. Web applications in the development phase often have many security deficiencies, and if these shortcomings become public, the security of the entire server is being compromised. Especially if the application being tested works with all the privileges, which is a common practice.

Vieira et al. (2009) points out that the application of the web security scanner in order to find the vulnerability of web services is of great importance for improving security. Accordingly, the benefits and advantages of using a

vulnerability scanner are also highlighted: Easy and widely-used way to test applications searching vulnerabilities; Use fuzzing techniques to attack applications and perform thousands of tests in an automated way.

Also, in order to increase the security of the web servers, regular testing is required. Therefore, scanning a computer network and testing for potential vulnerabilities relies on tools and processes for scanning computer networks and network devices at vulnerability. These tools and resources should be included in the security policies of any organization whose business relies on the information system in order to detect potential gaps and vulnerabilities of the network in time, and later take security measures that will provide adequate protection of the information system that the organization expects and requests. Network administrators should periodically run network vulnerability and penetration tests to help them detect network security failures that can compromise important information or devices, or even destroy malware.

3. NESSUS - A CASE STUDY

One of the most popular programs in the group of vulnerability scanners is Nessus. It can be implemented on Linux, FreeBSD, Solaris, Mac OS X 10.4 and 10.5 and Microsoft Windows operating systems. Its basic task is to detect known security flaws when analyzing the vulnerability by automating the process. To version 3.h Nessus was completely open source text, which is no longer. However, 3.h. version is available for free downloading and personal use. At an additional charge, which according to the license is mandatory for any commercial use, some additional benefits are implied. Nessus is reflected in the flexibility of the vulnerability assessment system. All required scanning tasks are executed via client-server, which makes Nessus architecture. An arbitrary number of servers that are placed on strategic locations inside or outside the target network, as well as the parallel control of each client's client (they can be more and different located), is enabled by architecture. Each request can be adjusted to the scan location. For example, an organization has a number of addresses that are public on the Internet, as well as their own - private subnets with address formats 192.168.x.y / 24. The first 24 bits indicate the network address, and as each segment is an 8-bit positive number, changing the field indicated by "x" within the limits 0 to 255 gives 256 possible subnets, each of which can have 254 cells. The Nessus architecture, organized through a client server, allows one server to be set up for each subnet of 254 cells, while at the same time a scan can be performed. (Archibald et al., 2015; Rogers, 2011, Beale et al., 2004).

Installing Nessus on a Windows computer results in five programs that make up the package. They are available via the Start menu and they are (Tenable, 2018):

- Plugin Update - There are special modules through which is implemented checks and scanning. The modules are in the form of text files whose script content is written in NASL: scripting language (Nessus Attack Scripting Language). Plugin Update is a program that takes care of the availability of all known server component verification, and the update of the vulnerability database starts with its launch.;
- User Management – is the program that is designed to manage users and serves to add user accounts that will have access to the scanner. A certificate is specified - username and password, depending on the method chosen for user authentication. It should be noted absurd failure: user account can be created and deleted, but cannot be modified. Although this is not a big problem because it is short for the installation of a user's computer;
- Product Registration - this program performs a scanner registration by receiving the registration code and executing it on the manufacturer's side. Registration unlocks or locks some of the features of the Nessus scanner, depending on the model. The version of this program in the home version is weakened and denied for some features such as checking the station deployment with a security policy, as well as the inaccessibility of some checking groups;
- Nessus Server Configuration - an IP address is set up and an access point where the server will respond, as well as an option to automatically update the vulnerability database at a twenty-four-hour level;
- Nessus Client.

Security warnings before installation - As a rule, Nessus is installed and managed using HTTPS and SSL support and using portal 8834, and the usual Nessus installation uses a self-signed SSL certificate.

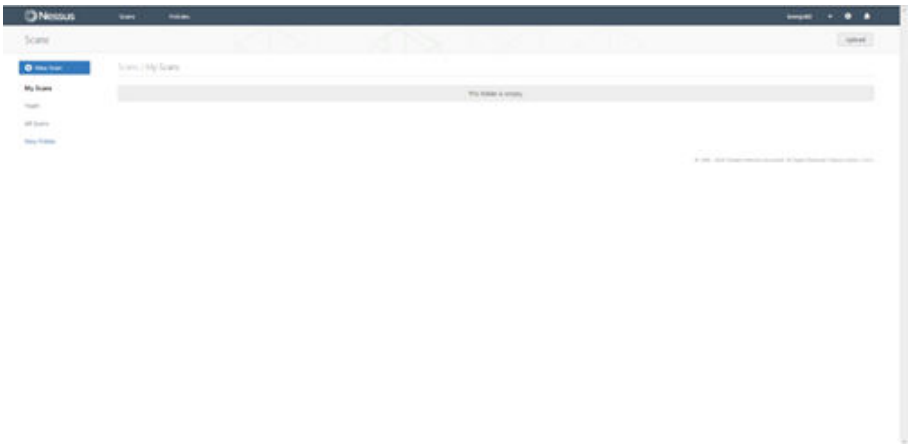
This section will not show the installation of Nessus and the registration of Nessus products.

Setting up and running a scan policy

Scan session - defines the Nessus client by selecting a check of certain vulnerabilities and scanning parameters through the client application, such as the type of scanner access, the number of concurrent checks and other

configuration options. The initial scan was followed by intuition, a Scan page is provided by scanning and running, and a page that views the report.

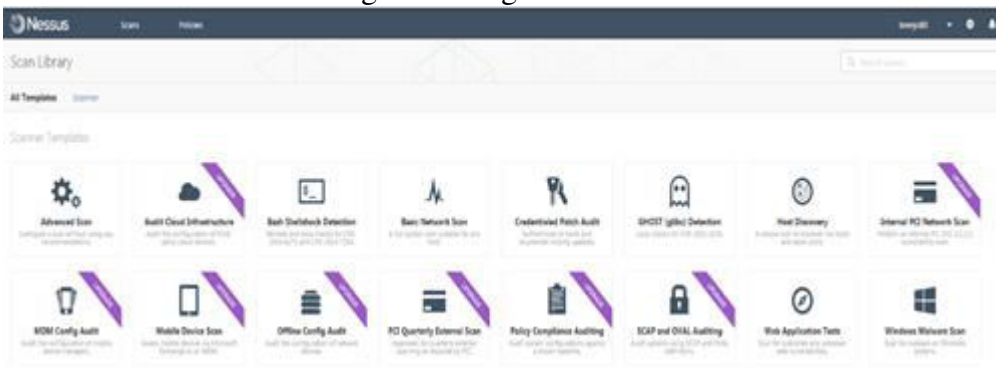
Figure 1. The original Nessus interface



Cells/stations that need to be scanned or network input are executed on the left side, which starts with "+" located in the lower left side and exists in several formats:

- **Single host** – entry of one IP address or DNS (or NetBIOS) name;
- **IP Range** - a range is entered which includes the start and end IP address.
- **Subnet** - the network and the net mask are entered;
- **Hosts in file** - selects a file listing the IP addresses or station names

Figure 2. Plugin selection



Which Nessus scanner will be used, is selected on the new screen (which, in addition to listed servers, provides the ability to add, delete, and modify the server list) by using the Connect button. The list of scanning policies can be modified and deleted and added to new ones is enabled after connecting to

one of the servers. Scanning of selected stations is done by clicking the Scan Now button once the policy is selected. The pages that are offered, which are contained in the screen for editing the scan policy, are:

- **Policy** - on this page are set: name and durability of the policy, the way in which the password is saved for the authorizations.
- **Options** - Base scan parameters, such as number of concurrent tests, number of scans for simultaneous scanning, disk scanning, accesses, and access scanners used, are on this page.
- **Credentials** - the user name and password, which the scanner is used for when scanning, are entered on this page. In addition, authentication mechanisms are: Windows credentials; SSH settings; Oracle settings; Kerberos configuration and authentication and Cleartext protocol settings.
- **Plugin selection** - the selection of tests to perform is performed on this page. Tests are formed through groups, all can be selected and can only be selected.
- **Network** - includes functions that control the consumption of network resources (the number of concurrent TCP sessions and the response time of the network activity).
- **Advanced** - the configuration parameters of the individual present tests and the dynamics of the selected tests make up this page. In addition, it contains certain configuration sections, such as the choice of scanning sensitive devices (such as printers) and user names and passwords of certain services (web, FTP, etc.).

After setting and selecting all the tests, by clicking the Save button, the policy is saved and started. After scanning, the report is grouped according to the IP addresses of the scanned resources and appears on the Report page. The report is unreliable for filtering according to the text within the results, so the criticality score may have the following levels:

- **High** - represents a security hole and it is assumed that the system is very vulnerable.
- **Medium** - presents vulnerabilities that do not pretend to become problematic.
- **Low** - is not considered vulnerable.

4. CONCLUSIONS

Before presenting the concluding observations should be compared also current vulnerability scanner such as the Retina with Nessus. Maybe Retina is better than Nessus in the domain of interface and reporting. What is the advantage of Retina is the functionality of a different set of solutions that are offered, the look is more tempting, and however, both solutions give a similar

set of functionality when they are paid. On the other hand, Nessus offers a number of free versions, which are not available in Retina. For reliability and precision, superior offers and multiple awards are distinguished by both these tools. Some statistics show that precision is more prevalent in Retina, the other with Nessus. Nessus has proven to be better at the speed of work with the default settings. When it comes to performing a quality vulnerability assessment - there is no prevailing one, both show the bandwidth of the network and the severity of the security protection walls over which it passes. It can be concluded that both tools are very powerful, quality and flexible. The methodology described is very well adjusted, and for wider solutions also offer technical possibilities, which is important. Nessus is a very powerful tool whose basic characteristics are flexibility and adaptability, and besides the very suitable server-client architecture and quality workmanship, the current look is conditioned by the former open source text and today belongs to Tenable products. Nessus's progress has provoked the first factor - a good idea has grown into the most demanding security analyzer with strong domination in that field. The development of Nessus has contributed, through suggestions and error messages, to a broad user base. Security is no longer a neglected activity in a world where network and network computing has already become an inevitable part of everyday life and business, precisely for this reason and for the improvement of security, scanners of vulnerability are getting more and more important.

REFERENCES

1. Archibald, N., Ramirez, G., Rathaus, N., Burke, J., Caswell, B., & Deraison, R. 2015. Nessus. Snort, & Ethereal Power Tools: Customizing Open Source Security Applications, First Edition, Rockland, Syngress.
2. Beale, J., Deraison, R., Meer, H., Temmingh, R., & Walt, C. V. D. 2004. Nessus network auditing. Syngress Publishing.
3. Hug, G., & Giampapa, J. A. 2012. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on Smart Grid*, 3(3), 1362-1370.
4. Krštenić, A. 2016. The application of cyber intelligence analysis in countering contemporary challenges, risks and threats. II međunarodna naučno-stručna konferencija bezbednost i krizni menadžment – teorija i praksa bezbednost za budućnost – 2016, pp. 171-177.
5. Morein, W. G., Stavrou, A., Cook, D. L., Keromytis, A. D., Misra, V., & Rubenstein, D. 2003 October. Using graphic turing tests to counter automated DDoS attacks against web servers. In Proceedings of the 10th ACM conference on Computer and communications security (pp. 8-19). ACM.

6. Rogers, R. (Ed.). 2011. Nessus network auditing. Elsevier.
7. Vieira, M., Antunes, N., & Madeira, H. 2009. Using web security scanners to detect vulnerabilities in web services. In Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on (pp. 566-571). IEEE.
8. Von Solms, R., & Van Niekerk, J. 2013. From information security to cyber security. Computers & Security, 38, 97-102.
9. Tenable, 2018. *Nessus Professional* [online] Tenable, Available at: <http://www.tenablesecurity.com/nessus/> [Accessed 28 April 2018].
10. Acunetix, 2018. *Web Server Security and Database Server Security* [online] Acunetix, Available at: <https://www.acunetix.com/websitesecurity/webserver-security/> [Accessed 20 April 2018].

Received: 14 June, 2018
Accepted: 23 June, 2018