Journal scientific and applied research, vol. 4, 2013
Association Scientific and Applied Research
International Journal

Original Contribution ISSN 1314-6289

USING THE SECURITY NETWORK SCANNER GFI LANGUARD TO DISCOVER AND IMPROVE THE VULNERABILITIES IN THE COMPUTER NETWORK SYSTEMS

Petar Boyanov

KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR.

e-mail: peshoaikido@abv.bg

Abstract: *In this paper a comprehensive testing for computer network vulnerabilities is made. Thanks to the program product GFI LanGuard some critical flaws and vulnerabilities have been discovered and thereby this action improves the security mechanisms in the tested hosts. It is recommended that many cyber-security professionals and IT administrators to use GFI LanGuard in order to increase the computer and network security in their organizations.*

Key words: *Patch management, Network auditing, Vulnerability assessment, Computer and network security.*

1. Introduction

The cyber-crimes influence huge damages on computer network systems. Every day many international companies, organizations and other institutions sustain losses because of critical flaws and vulnerabilities in their computer network systems. Therefore the security professionals and IT administrators must find a solution to decrease the vulnerabilities and improve the security mechanisms against various malicious cyber-attacks.

Previous technical papers presented different investigations and results before and after the implementation of software product GFI LanGuard. In this paper some sophisticated researches for flaws and vulnerabilities in several hosts on WLAN (Wireless Local Area Network) are made in order to analyze the risk and to increase the security level of these hosts. Thanks to the achieved results many security professionals could detect the different types of vulnerabilities and implement new comprehensive and strong security mechanisms. The new achievement in this paper is that some recommendations for specific security patches and software programs are made in order to improve the security level of the hosts.

This paper is structured as follows. First, in section 2, the comparative analyzes of the security network scanner GFI LanGuard are

made. After that, in section 3, the comprehensive discovering and improving of the vulnerability level of host 1.1.1.11 is accomplished. The achieved results after configuring security are presented in section 4. The final conclusions and recommendations are made in section 5.

2. Related work

In [1] the state transition model of GFI LanGuard for intrusion detection systems by d'Auriol and Surapaneni is illustrated. The implementation of program software GFI LanGuard with operating system BackTrack is presented by Nelson, Phillips and Steuart [4]. In [5] only common explanations and characteristics of the network security scanner GFI LanGuard by Shimonski are made. In [3] different comparative investigations with Nessus and GFI LanGuard in a specific network by Hamedani and Skaria are made.

3. Experiment

This experiment in a WLAN of 15 hosts in computer laboratory in the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen is made. Each host uses a wireless N USB Adapter TL-WN721N 150Mbps. In this computer laboratory a Wireless N Router TL-WR741ND 150Mbps is used. In the wireless router the DHCP (Dynamic Host Configuration Protocol) is activated in order to receive each host automatically IP (Internet Protocol), network mask, default route address and DNS server address. The WLAN uses 24-bit network mask and the network ID is 1.0.0.0, i.e. 1.0.0.0/24.

GFI LanGuard is a network security scanner that can implement a patch management, network auditing solution and vulnerability assessment. The aim of patch management is to fix vulnerabilities before the cyber-criminals to implement different malicious cyber-attacks and this software product has the ability for automatic download and remote installation of patches and service packs for Microsoft Windows and MAC operating systems as well as other third-party operating systems and applications [2]. Thanks to the vulnerability assessment GFI LanGuard can discover the malicious threats early through vulnerability check databases such as OVAL (Open Vulnerability and Assessment Language), CVE (Common Vulnerabilities and Exposures) and SANS Top 20 [2]. This program product has the ability to audit and proof all software and hardware components on the selected computer network, to illustrate a common picture of installed applications and hardware on the host, to measure the level of security applications like a antivirus and firewalls, to present the open TCP and UDP ports and to show any shares and services running on the remote hosts [2].

The used software in this paper has 30-day trial license and has the ability to scan up to 25 IP addresses. The version of this product is 11.1 and the build is 20121127.

The IP address range begins from 1.1.1.2 to 1.1.1.15. The

summary of scan results generated during the hosts audit shows that only 11 hosts are in active state and the vulnerability level for the scanning session is **high** (fig. 1)**.**

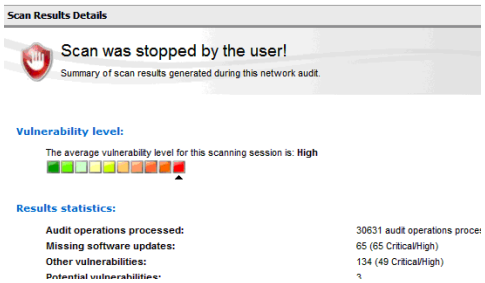

Fig. 1. The scan results details.

The result statistics shows the following items:

- Audit operations processed: 30631 audit operations processed;
- Missing software updates: 65 (65 critical/high);
- Other Vulnerabilities: 134 (49 critical/high);
- Potential vulnerabilities: 3;
- Installed applications: 88 (0 unauthorized);
- Open common ports: 78;
- Total scan time: 36 minutes, 30 seconds;
- Average scan time per machine: 7 minutes, 6 seconds.

The vulnerability level on host with IP address 1.1.1.11 is **high.** The computer name of this host is PESHOSAN_ and uses operating system Microsoft Windows 7 Ultimate. Additionally the vulnerability assessment for this host presents the following items:

- High security vulnerabilities - 36;
- Medium security vulnerabilities - 22;
- Low security vulnerabilities - 38;
- Potential vulnerabilities - 3;
- Missing service pack and updates rollups - 4;
- Missing security updates - 1.

The other hosts don't have vulnerabilities and therefore the whole attention is pointed to decrease the vulnerability level of this host and to improve his security level. On fig. 2 is shown the current vulnerability level for the all hosts in the WLAN.

Fig. 2. The vulnerability level of the hosts in the WLAN.

Other flaw for this host is the malware protection. On fig. 3 is shown the list of malware issues for current host 1.1.1.11.

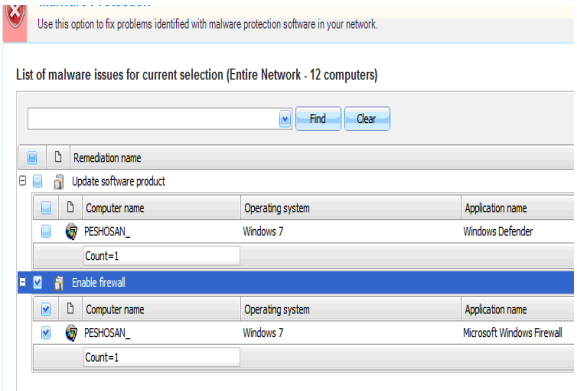

Fig. 3. The malware protection for the host - PESHOSAN_

This figure shows that the applications Windows Defender and Microsoft Windows Firewall must be instantly updated.

The Vulnerability level and security sensors for host with IP address 1.1.1.11 are shown on fig. 4. This figure presents that it has the highest vulnerability level.

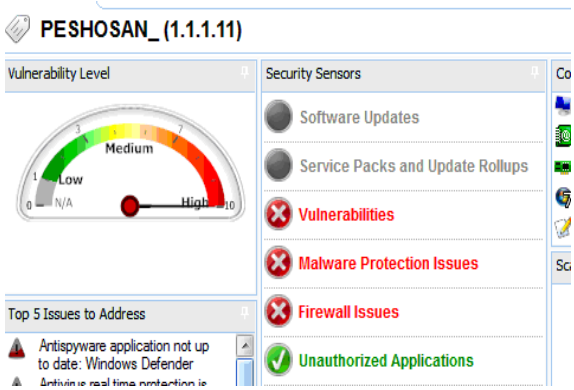

Fig. 4. Common vulnerability assessment for host 1.1.1.11

First, in this host must be updated the application Windows Defender (fig. 5).

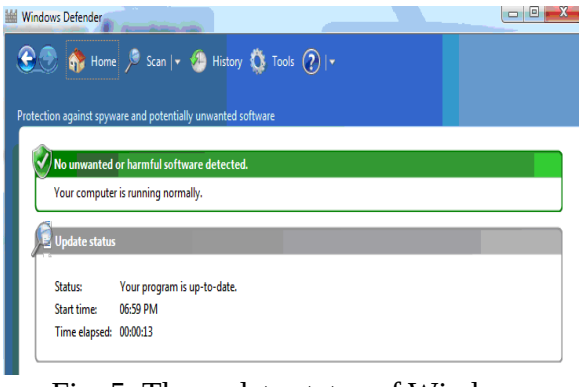

Fig. 5. The update status of Windows Defender.

The next step is to be updated the adobe flash player with the latest version - 11.8.800.94. It is recommended to be installed this version, because the last other are very vulnerable against cyber-attacks. Adobe shockwave player must be also updated with the latest version - 12.0.3.133. The web application adobe air 3.8 is installed on the host. The Microsoft Windows Firewall is enabled and ready to protect the incoming and outgoing network connections. Each installed software product must be updated with latest version.

4. Results

After the configuration for this host has made, the whole WLAN has been scanned and tested once again against vulnerability and flaws in hosts. The summary of scan results generated during the hosts audit is shown in fig. 6.

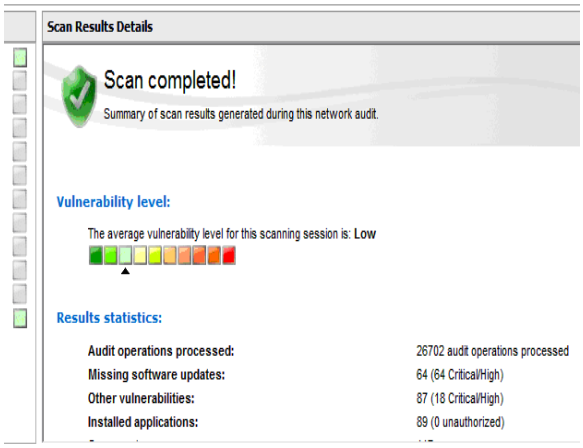

Fig. 6. The scan results details after the new security configuration.

These results show that the average vulnerability level for the scanning session is **Low** and the results statistics show the following items:

- Audit operations processed: 26702 audit operations processed;
- Missing software updates: 64 (64 critical/high);

- Other Vulnerabilities: 87 (18 critical/high);
- Installed applications: 89 (0 unauthorized).

Thanks to the achieved results the vulnerability level is decreased and the security level is improved (fig. 7).

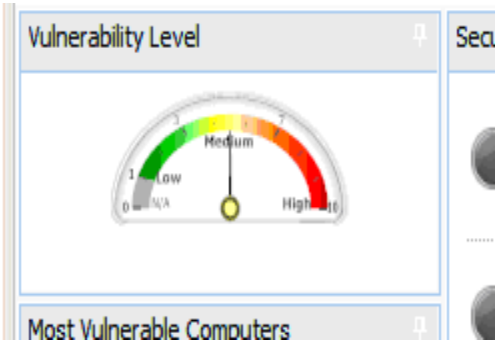

Fig. 7. The decreased vulnerability level of the hosts in the WLAN.

After the successfully installed patches the malware protection software for the host 1.1.1.11 is up to date and therefore this host is protected against various malicious cyber-attacks (fig. 8).

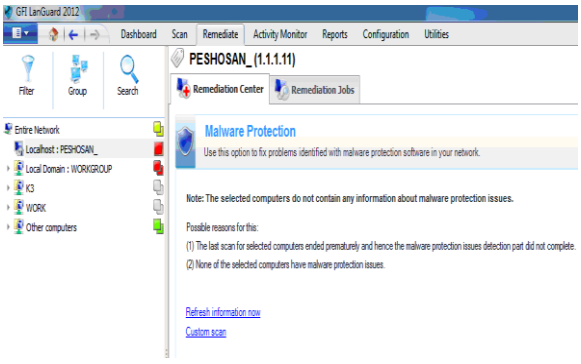

Fig. 8. The malware software protection for the host 1.1.1.11.

The vulnerability assessment level for host 1.1.1.11 illustrates that after the configuring security the different vulnerability types with 87% are decreased and thereby the security level and system performance of this host are improved (fig. 9).

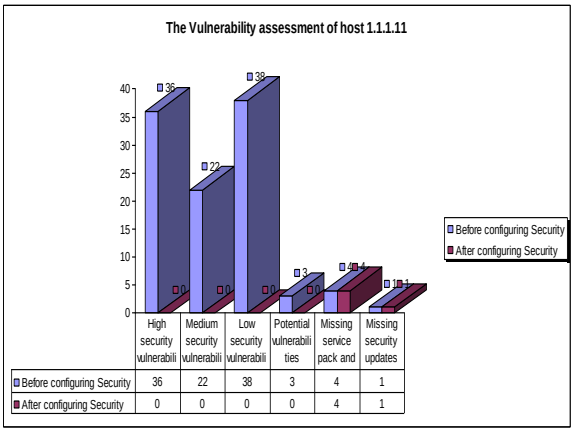

Fig. 9. The vulnerability assessment of host 1.1.1.11

5. Conclusion

In this paper a comprehensive discovering and improving the vulnerabilities in WLAN from several hosts is made. Thanks to the achieved results the configuring security level and system performance of host 1.1.1.11 have been improved with 87%. It is recommended to keep the different programs up-to-date in order to detect and prevent malicious cyber-attacks. The most important programs that must be updated are adobe air, adobe reader, flash player plugin, google chrome, mozilla firefox, internet explorer, java runtime environment, uTorrent and etc. In order to be secured each host it is recommended for the security professionals and IT administrators to use network security scanners for discovering and fixing the flaws and vulnerabilities in the computer network systems against various malicious cyber-attacks.

Acknowledgements

This paper is supported by the Project BG051PO00l-3.3.06-0003 "Building and steady development of PhD students, post-PhD and young scientists in the areas of the natural, technical and mathematical sciences".

The Project is realized by the financial support of the Operative Program "Development of the human resources" of the European social found of the European Union.

References:

[1] d'Auriol B. J., & Surapaneni K., A State Transition Model Case Study for Intrusion Detection Systems. In Security and Management, June 2004, pp. 186-192

[2] GFI LanGuard,Documentation, Datasheet/Brochure, Available at http://www.gfi.com/~/media /Files/Datasheets/LANSS/GFILanGuardBrochureA4_EN_GEN.pdf

[3] Hamedani A. R. F., & Skaria S., Network Security Issues, Tools for Testing Security in Computer Network and Development Solution for Improving Security in Computer Network, Technical report, IDE1012, Halmstad University, February 2010

[4] Nelson B., Phillips A., & Steuart C., Guide to computer forensics and investigations, 2010, Available at http://www.CengageBrain. com

[5] Shimonski R. J, Threats and your Assets–What is really at Risk?, 2004, Available at http://leetupload.com/database/Misc/Papers/Asta%20la%20Vista/threats_and_your_assets_%E2___what_is_really_at_risk.pdfhttp://windowsecurity.com/pages/article_p. asp, 82-89