ISSN 2278-3091
Volume 9 No.2, March - April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse182922020.pdf
https://doi.org/10.30534/ijatcse/2020/182922020

Automation of information security audit in the Information System on the example of a standard "CIS Palo Alto 8 Firewall Benchmark"

Petr Perminov[1], Tatiana Kosachenko[2], Anton Konev[3], Alexander Shelupanov[4]
[1] Tomsk State University of Control Systems and Radioelectronics, Positive Technologies, Russian Federation, ppv@fb.tusur.ru
[2] Tomsk State University of Control Systems and Radioelectronics, Russian Federation, 6takos9@gmail.com
[3] Tomsk State University of Control Systems and Radioelectronics, Russian Federation, kaa1@keva.tusur.ru
[4] Tomsk State University of Control Systems and Radioelectronics, Russian Federation, saa@tusur.ru

ABSTRACT

Nowadays cyber security issues have a significant value in the world. Due to the constant increase in the number of cyberattacks, the security issues of network infrastructure are of particular relevance. For leading manufacturers of information security tools, the issue of standardizing audit mechanisms is an urgent issue, but this is not enough for an organization to build a security system. To solve this problem, it is proposed to automate the process of standardizing firewall settings. This article analyzes the security standard "CIS Palo Alto Firewall 8 Benchmark" and offers a methodology for designing a network scanner for Palo Alto Networks devices, defines the requirements for the software implementation of the module for MaxPatrol 8.

Key words: CIS, MaxPatrol 8, Palo Alto, security standard, vulnerability scanner.

1. INTRODUCTION

Currently, ensuring the security of information systems is one of the most important tasks in the field of information technology. At the same time, much attention is paid to protecting the network infrastructure.

Palo Alto Networks is the largest manufacturer of network security systems, including software and hardware firewalls, for medium and large organizations. Such protection tools can significantly increase the level of security of the enterprise network, however, this requires the correct administration of these devices.

To check the correctness of device settings, security standards can be used that describe the necessary security policies, most often boiling down to a certain set of information system settings. These standards can be developed both independently by organizations and by third-party organizations working in the field of information security. Standards can be either public or private.

The nonprofit organization Center for Internet Security (CIS) develops global security standards for various systems, which are a recognized global standard and best practices for securing IT systems and data against attacks.

For Palo Alto devices, the standard Palo Alto 8 Firewall Benchmark was developed by CIS.Verification of compliance with the standard can be done either manually by a specialist, or using automated security analysis systems. Automated verification takes much less time, is less prone to errors due to the exclusion of the human factor, and also allows you to more conveniently track changes in the analyzed systems.

An example of an automated analysis system is the MaxPatrol 8 software product of Positive Technologies. The program is a network scanner that analyzes the security of information systems. The scanner supports three scan modes:

- PenTest;
- Audit;
- Compliance.

In Compliance mode, based on the data received from the system (system type, installed OS and its version, software list), the applicable safety standards are determined

2. LITERATURE REVIEW

According to the latest research in the third quarter of 2019, the proportion of attacks aimed at stealing information increased to 61% in attacks on legal entities and up to 64% in attacks on private individuals (versus 58% and 55% respectively in the second quarter), the number of vulnerabilities, which on average per web application, has decreased by half as compared to 2018. On average, there are 22 vulnerabilities per system, four of which are at high risk. The most common vulnerabilities associated with security misconfigurations.

Attackers are increasingly using scanning as a method to gather critical critical network information, which is used to further attack this network. Various authors propose as a counteraction: a clustering system for detecting attacks [1], transversal detection system [2], Z-Wave Misuse-Based Intrusion Detection System (MBIDS) [3], Network Intrusion Detection Systems (NIDSs) [4]. Many cybersecurity professionals prefer to use firewalls in their work. However, they are also prone to attacks, such as denial of firewalling (DoF) attacks [5], where attackers use carefully crafted traffic to efficiently overload the firewall.

The authors propose various methods for designing a firewall, such as Quality of Firewalling (QoF) [6], SCADAWall [7], techniques for reconstructing the firewall policy by intelligently choosing the probing packets based on the responses of previous probes [8], analytical dynamic multilevel early packet filtering mechanism to enhance firewall performance [9], extendible firewall monitoring tool that enables customers to probe their provider's filtering behavior [10]. However, all the construction methods we have reviewed are not suitable for automating the verification of Palo Alto Networks network devices.

To solve this problem, threat models for different types of networks were considered [11-16] after the analysis, a methodology for designing a firewall using the security standard CIS Palo Alto Firewall 8 Benchmark was built. This technique was developed for the MaxPatrol 8, system based on the XSpider professional vulnerability scanner. The scanner used in MaxPatrol 8 allows you to quickly detect open ports, network nodes and server applications, as well as using heuristic analysis mechanisms to identify the level of network security.

3. CIS PALO ALTO FIREWALL 8 BANCHMARK ANALYSIS

The standard is a set of grouped security requirements for the analyzed system. The result of checking the system according to the standard is a final score and a list of requirements with marks on their compliance with the target system.

The standard includes terms of use, overview, set of requirements and two applications: a table template with final results and a history of changes to the standard.

The overview contains typographical conventions, profile definitions and scoring information. According to this, each requirement is «Scored» or «Not Scored». Information about this is in the title of the requirement.

«Scored» requirements increase the total score when the system conforms to them and decrease the score when non-compliant. «Not Scored» requirements do not affect the final score.

Two profile definition are described:
– level 1. This profile includes basic security settings that provide an obvious increase in security, do not reduce system performance;
– level 2. This profile includes more specific requirements that provide a higher degree of security, but may adversely affect the performance or functionality of the system.

Requirements can be applied to both levels at the same time.

Each requirement includes the following items:

– Profile Applicability;
– Description;
– Rationale;
– Audit;
– Remediation;
– Default Value;
– References;
– CIS Controls.

Also, some requirements include the Impact clause.

4. SOFTWARE IMPLEMENTATION

The collection of primary information is carried out using the built-in MaxPatrol module by connecting to the scanned machine via SSH. The contents of the files and command output are collected by successive system calls. At the same time, a number of commands proposed by the CIS standard have been optimized in order to minimize the execution of commands on the target system. For example, in case of multiple accesses to the file or to the output of a command from different controls, the contents of the file or the output of the command will be requested only once, which positively affects the scan time of the target system (Fig. 1). It should be understood that the data obtained in this way may constitute a commercial secret, therefore, after scanning, this information is not saved anywhere.

After connecting to the system via SSH, it is necessary to configure message output formats in such a way that the following conditions are met:

– the output format was not configuration dependent;
– noninteractive (automated) interaction was possible;
– the minimum amount of information was transmitted;
– the minimum number of SSH requests was executed.

Palo Alto network devices have the ability to display information in the following formats:

– standard view;
– XML;
– set. It is a set of commands necessary to set the current configuration;
– JSON.

For automated processing, it is more convenient to use machine-oriented JSON and XML formats, however, there were some problems with them:

– the output of some commands in the JSON format turned out to be incorrect, and an error occurred when trying to deserialize it, which is why it was not justified to use it for automated processing;
– XML command output contains a large amount of redundant overhead information, and the data structure after deserialization is inconvenient for further processing and may depend on the system settings. Also, there is no full XML support in the MaxPatrol 8 scan scripts.

As a result, it was decided to use standard data output and implement a processor for it, at the output of which the required data structure will be generated. After executing the commands, their output is processed and stored in the general data structure. The simplified process of converting the system configuration to the internal view is presented in Figure 2 as IDEF0.

To check the compliance of the parameters, a set of comparison functions is used. In general, the following parameters come to the input of functions:

– desired value or list of values;
– current system value;
– comparison operation;
– the name of the parameter to display in the table;
– default parameter value;
– the result of the previous check.

The result of the function is a structure that includes the status of the verification taking into account previous checks and a table with the results.

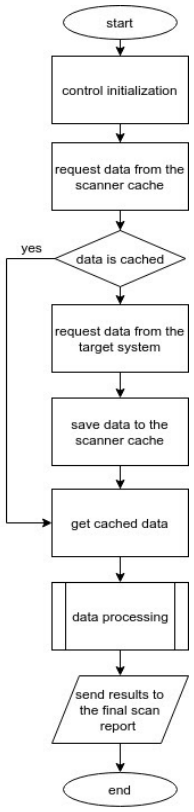

Figure 1: Collection and preprocessing algorithm

All values of parameters:

- any value is allowed;
- only an empty value is allowed;
- any nonempty value is valid;
- mathematical comparison operators (=, ≠,>, ≥, <, ≤);
- is between two values.

The following operations are allowed to compare string values of parameters:

- any value is allowed;
- only an empty value is allowed;
- any nonempty value is valid;
- equal to one of the given values;
- contains one of the specified lines;
- does not contain any of the specified lines;
- starts with one of the specified values;
- does not start with any of the specified values;
- ends with one of the specified values;
- does not end with any of the indicated values;
- Satisfies one of the given regular expressions;
- does not satisfy any of the given regular expressions;
- there is an occurrence of one of the given regular expressions;
- no occurrences of any of the given regular expressions;
- there are occurrences of all given regular expressions.

The following options are valid for comparing lists:

- any value is allowed;
- only an empty list is allowed;
- any non-empty list is acceptable;
- equal to the specified list;
- may contain only the indicated elements;
- may not contain any of these elements;
- must contain any of these elements;
- must contain all the specified elements;
- may contain only the specified elements specified by the regular expression;
- cannot contain elements specified by a regular expression.

For comparison, enumeration type comparison function is not used. The strict correspondence of the set value to the system is checked. To disable the check, the service value "Any value" is used.

The overall process is depicted in Figure 2.

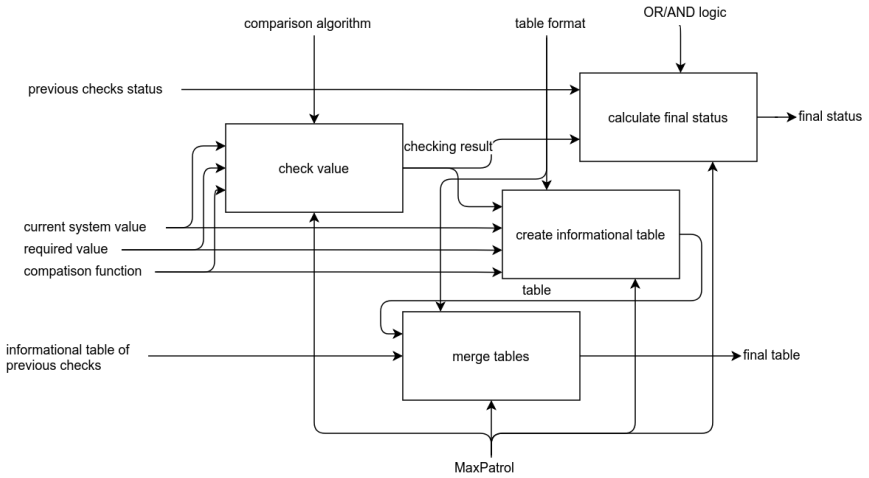

Figure 2: The general process of verifying an individual requirement

5. CONCLUSION

A methodology for designing a scanner for a firewall was proposed, and a module was implemented to automate verification for Palo Alto Networks network devices. As a result of the analysis of the results obtained, it was revealed: the required time for inspections is reduced, the load on employees involved in servicing networks of automated systems to conduct checks for compliance with safety standards. Manual verification of compliance with the standard can take several hours to test a single device once, while automated scanning can take several minutes, and can also be performed simultaneously for several systems. In addition, the reliability, information content of inspections and the relevance of the results of conformance checks are also increased due to the possibility of launching according to a schedule or according to specified scenarios.

Due to automation of the scanning process and regular analysis of information systems, it is possible to track changes in them and timely detect violations of the correct functioning of both individual subsystems and systems as a whole.

The module that implements the standard was introduced as part of the Positive Technologies MaxPatrol 8 product.

ACKNOWLEDGEMENT

This research was funded by the Ministry of Science and Higher Education of Russia, Government Order for 2020–2022, project no. FEWM-2020-0037 (TUSUR).

REFERENCES

1. Sabottke, C.; Chen, D.; Layman, L.; Dumitras, T. **How to trick the Borg: threat models against manual and automated techniques for detecting network attacks.** *Computers and Security*. Volume 81, March 2019, Pages 25-40. https://doi.org/10.1016/j.cose.2018.07.022
2. Serrano Mamolar, A.; Pervar, Z.; Alcaraz Calero, J.M.; Khattak, A.M**. Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks**, *Computers and Security*. Volume 79, November 2018, Pages 132-147.
3. Fuller, J.D.; Ramsey, B.W.; Rice, M.J.; Pecarina, J.M. **Misuse-based detection of Z-Wave network attacks**. *Computers and Security*. Volume 64, 1 January 2017, Pages 44-58. https://doi.org/10.1016/j.cose.2016.10.003
4. Cerroni, W.; Moro, G.; Pasolini, R.; Ramilli, M. **Decentralized detection of network attacks through P2P data clustering of SNMP data**. *Computers and Security*. Volume 52, 1 August 2015, Pages 1-16. https://doi.org/10.1016/j.cose.2015.03.006
5. Liu, A.X.; Khakpour, A.R.; Hulst, J.W.; Ge, Z.; Pei, D.; Wang, J. **Firewall fingerprinting and denial of firewalling attacks.** *IEEE Transactions on Information Forensics and Security*. Volume 12, Issue 7, July 2017, Pages 1699-1712. https://doi.org/10.1109/TIFS.2017.2668602
6. Xu, J.; Singhal, M. **Design of a High-Performance ATM Firewall**. *ACM Transactions on Information and System Security*. Volume 2, Issue 3, 1 August 1999, Pages 269-294. https://doi.org/10.1145/322510.322520
7. Li, D.; Guo, H.; Zhou, J.; Zhou, L.; Wong, J.W. **SCADAWall: A CPI-enabled firewall model for SCADA security**. *Computers and Security*. Volume 80, January 2019, Pages 134-154. https://doi.org/10.1016/j.cose.2018.10.002
8. Ali, M.Q.; Al-Shaer, E.; Samak, T. **Firewall policy reconnaissance: Techniques and analysis.** *IEEE Transactions on Information Forensics and Security*. Volume 9, Issue 2, February 2014, Pages 296-308.
9. Trabelsi, Z.; Zeidan, S.; Masud, M.M.; Ghoudi, K. **Statistical dynamic splay tree filters towards multilevel firewall packet filtering enhancement**. *Computers and Security*. Volume 53, 10 July 2015, Pages 109-131. https://doi.org/10.1016/j.cose.2015.05.010
10. Ullrich, J.; Cropper, J.; Frühwirt, P. **The role and security of firewalls in cyber-physical cloud computing**. *Eurasip Journal on Information Security*. Volume 2016, Issue 1, 1 December 2016, 18.
11. Shelupanov, A.; Konev, A.; Kosachenko, T.; Dudkin, D. **Threat Model for IoT Systems on the Example of OpenUNB Protocol.** *International Journal of Emerging Trends in Engineering Research*. Volume 7, no. 9, 2019, Pages 283-290. https://doi.org/10.30534/ijeter/2019/11792019
12. Novokhrestov, A.; Konev, A.; Shelupanov, A. **Model of Threats to Computer Network Software.** *Symmetry*. Volume 11, Issue 12, 2019, 1506.
13. Shelupanov, A.; Evsyutin, O.; Konev, A.; Kostyuchenko, E.; Kruchinin, D.; Nikiforov, D. **Information Security Methods – Modern Research Directions.** *Symmetry*. Volume 11, Issue 2, 2019, 150. https://doi.org/10.3390/sym11020150
14. Novokhrestov, A.; Konev, A.; Shelupanov, A.; Buymov, A. **Computer network threat modelling.** *Journal of Physics Conference Series.* 1488 (2020), 012002.
15. Mahalakshmi, S.; Dr. Latha, R., **Artificial Intelligence with the Internet of Things on Healthcare systems: A Survey** *International Journal of Advanced Trends in Computer Science and Engineering.* Volume 8, No.6, November-December 2019, Pages 2847-2854. https://doi.org/10.30534/ijatcse/2019/27862019
16. Siwoo Byun, **Gateway-based Resource Control for Reliable IoT Environments** *International Journal of Advanced Trends in Computer Science and Engineering.* Volume 8, No.5, September-October 2019, Pages 1881-1885. https://doi.org/10.30534/ijatcse/2019/11852019