DOI 10.34054/bdc002

EXTRACTION, INTEGRATION AND DATA PROCESSING IN THE SIEM «SPLUNK» USING «NESSUS» VULNERABILITY SCANNER

Petro Venherskyi,

Professor, Department of applied mathematics and informatic, Ivan Franko National University of Lviv, Ukraine

Roman Karpiuk,

Security Analyst, SecOps Team, SoftServe Inc, Lviv, Ukraine

Promote Ukraine

Conference proceeding

Behind the Digital Curtain. Civil Society vs State Sponsored Cyber Attacks

Brussels - 25/06/2019
DOI 10.34054/bdc000

In this work we propose: creating an integrated environment between the Nessus vulnerability scanner and Splunk's security information and event management system; development of analytics for the help of information security specialists to develop and analyze vulnerabilities discovered in systems.

The urgency of the topic lies in the fact that the standard methods that provide the individual SIEM "Splunk" or the vulnerability scanner "Nessus" is not enough for the complete review of problems in the system and as a consequence of the implementation of a specialist in analyzing and making the necessary decisions. The practical relevance is to properly integrate these two products, as well as develop a unique analytics for quick and easy analysis.

Key words: information and security management system, vulnerability scanner, security event management, Splunk system, Nessus scanner.

I. Introduction.

Currently, more and more attention is being paid to ensuring the security of information in large institutions and companies, as well as in medium and small organizations. Objects that protect different levels of access, all kinds of deployment of computing environments and various topology network interactions. The task of providing security through universal means of detecting and preventing attacks is complicated, including due to the rapid increase in the number of users and a variety of types of devices, the use of cloud technologies and multiple increases in the volume and speed of transmission and processing of information. One of the classes of tools that enables the security of systems of any level and set of devices is the information and security management system (SIEM). The advantage of these solutions lies in a flexible approach when implementing and independent of the set of specifications and platforms for the ultimate protected infrastructure.

I. Vulnerability Scanners.

Vulnerability Scanners are software or hardware tools for diagnosing and monitoring networked computers that scan networks, computers and programs to detect possible security issues, evaluate and eliminate vulnerabilities.

Vulnerability scanners allow you to check various applications in the system for the presence of a "guillotine" that can be used by traps. Low-level tools, such as port scanners, can also be used to detect and analyze possible applications and protocols that run on the system. (https://www.tenable.com./products/nessus/nessus-professional, General Information, main page about sub-product)

II. Security Information and Event Management.

SIEM (security information and event management) is a combination of two terms that indicate the scope of application software: SIM (Security information management) - information security management and SEM (Security event management) - management of security events. SIEM technology provides real-time analysis of security events (alarms) coming from network devices and applications. SIEM is represented by applications, devices or services, and is also used to log data and generate reports for compatibility with other business data. The term itself was invented by Gartner in 2005, but since then the very concept and all that belongs to it, has undergone many changes. (https://www.splunk.com, General Information, main page).

III. Integration.

As a vulnerability scanner, we used the product from Tenable Company Nessus[2] (https://www.tenable.com./products/nessus/nessus-professional, General Information, main page about sub-product). As an SIEM system - "SPLUNK" [1] (https://www.splunk.com/, General Information, main page).

1. First of all, we need to install Splunk's special application (add-on) - "Splunk Add-on for Tenable", This application allows you to interact with Spline from Nessus, that is, it contains all the necessary scripts for the correct work

2. The second step is to generate keys for API access to Nessus-a. To do this, you need to generate two keys "Access Key" and "Secret Key" on the scanner itself

3. Next in Splunk, you need to create an index that will record (index) the data coming from the vulnerability scanner.

4. After creating the index, you must add the input parameters (inputs) in the already installed application for Nessus. This is where we need pre-generated access keys.

For a more detailed description of the manual, use the official documentation: https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/integrations/How_To_Guide_Splunk_v2.pdf.

After receiving two "portions" of data there is a completely logical question - "And how do we combine these data?". After all, if these data are different then there is no use for them for analytics. We will return to this question a bit later. But I suppose I need to realize that all the data that is received by Splunk is reliable.

After analyzing the data obtained at Splunk-u with the results on Nessus-I, we see one, however, extremely critical non-conformance. Splunk does not receive the “Plugin Output” field. This field is extremely important because it includes where the vulnerability was detected, and may also contain local recommendations for addressing certain vulnerabilities.

It’s not hard to guess that the problem with the appliance that extracts data for Splunk.

So, after the study, a weak spot was found. This is a python script called “nessus_data_collector.py”. All further corrections are indicated in the work.

After analyzing all the above, we can conclude that in order to assess the picture of information security, we must work on the vulnerability data in the system. Vulnerability scanners should be used to automate inspection and detection of inconsistencies. Although all the actual solutions for vulnerability scanners have their own, by default, standard data display system, however, for IT analysts it will be difficult to operate, analyze, and ultimately decide if these data are found in different “places” of sources. Also, to perform a certain auto-correlation of events to detect more advanced attacks in order to adjust them on time, it is very difficult almost impossible if the information is dispersed across different resources. Therefore, in this case, the Security Information and Event Management (SIEM) system should be used for storing and processing raw data.

So, during the implementation, we examined the functioning of SIEM systems and vulnerability scanners in general. Considered some of the best representatives of these security tools.

Have made a direct integration between the Nessus vulnerability scanner and the SIEM Splunk representative. However, our integration did not end at the level of simple data transmission, but were built on the progress of dashboards. Since “raw” data is difficult to process, the analyst will have to spend a fair amount of time searching for the information he needs. That is why it took a lot of time to implement the correct display of input data. This greatly simplifies the perception of information and enables a cybersecurity expert to timely process certain IS incidents, as well as monitor certain trends in vulnerability in the company and, accordingly, make / provide some analytics.

Our dashboards which provide some views of corporate vulnerabilities (Fig.1-4):

Fig. 1. Vulnerability (Corporate Resources). Part 1

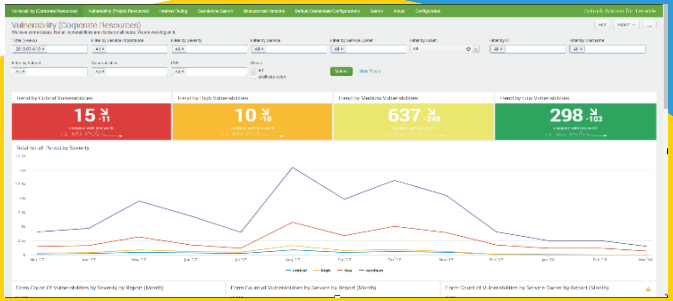

Vulnerability (Corporate Resources)
Trend by Critical Vulnerabilities
15 -11
Trend by High Vulnerabilities
10 -10
Trend by Medium Vulnerabilities
637 -249
Trend by Low Vulnerabilities
298 -103
Total for all Period by Severity
critical
high
low
medium

Fig 2. Vulnerability (Corporate Resources). Part 2

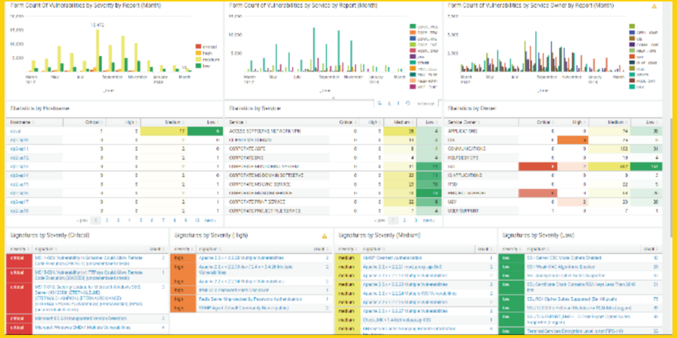
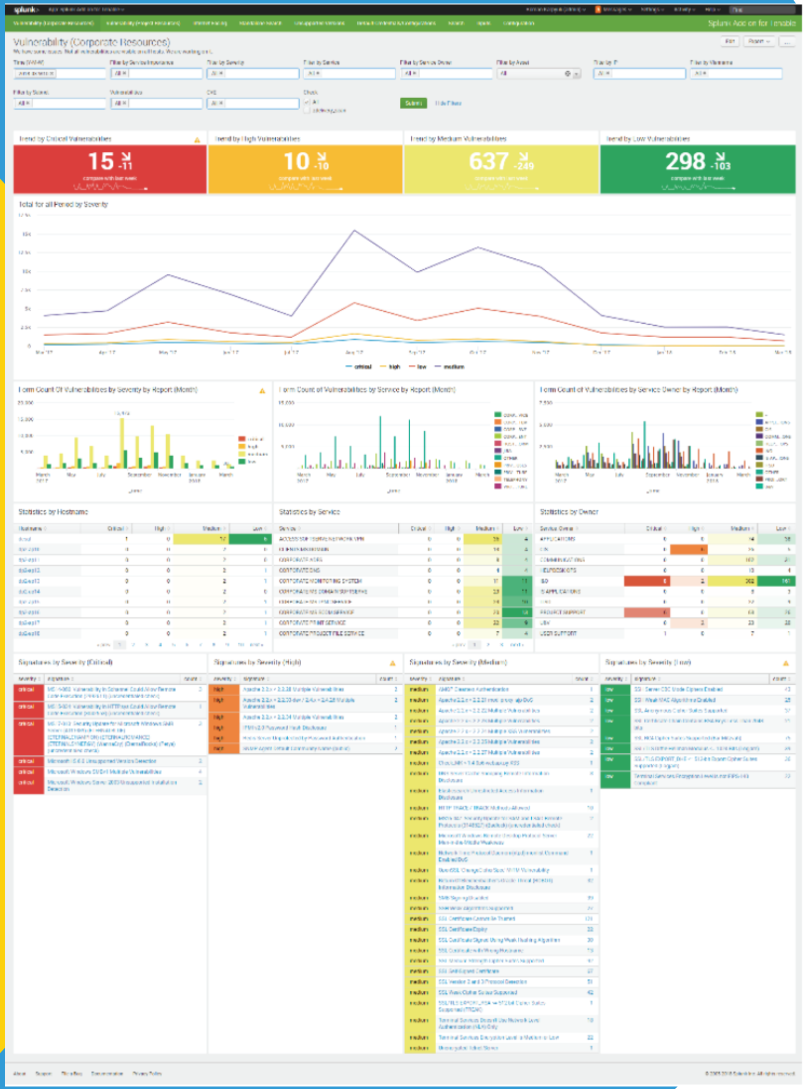

Form Count Of Vulnerabilities by Severity by Report (Month)
Form Count of Vulnerabilities by Service by Report (Month)
Form Count of Vulnerabilities by Service Owner by Report (Month)
Statistics by Hostname
Statistics by Service
Statistics by Owner
Signatures by Severity (Critical)
Signatures by Severity (High)
Signatures by Severity (Medium)
Signatures by Severity (Low)

Fig. 3. Vulnerability (Corporate Resources). Part 3

Signatures by Severity (Critical)
Signatures by Severity (High)
Signatures by Severity (Medium)
Signatures by Severity (Low)

Fig. 4. Vulnerability (Corporate Resources). General View.


splunk
Splunk Add on for Tenable
Vulnerability (Corporate Resources)
Submit
Hide Filters
Trend by Critical Vulnerabilities
15 -11
compare with last week
Trend by High Vulnerabilities
10 -10
compare with last week
Trend by Medium Vulnerabilities
637 -249
compare with last week
Trend by Low Vulnerabilities
298 -103
compare with last week
Total for all Period by Severity
critical
high
low
medium
Form Count Of Vulnerabilities by Severity by Report (Month)
Form Count of Vulnerabilities by Service by Report (Month)
Form Count of Vulnerabilities by Service Owner by Report (Month)
Statistics by Hostname
Statistics by Service
Statistics by Owner
Signatures by Severity (Critical)
Signatures by Severity (High)
Signatures by Severity (Medium)
Signatures by Severity (Low)

I. Conclusions.

After analyzing all the above, we can conclude that in order to assess the picture of information security, we must work on the vulnerability data in the system. Vulnerability scanners should be used to automate inspection and detection of inconsistencies. Although all the actual solutions for vulnerability scanners have their own, by default, standard data display system, however, for IT analysts it will be difficult to operate, analyze, and ultimately decide if these data are found in different “places” of sources. Also, to perform a certain auto-correlation of events to detect more advanced attacks in order to adjust them on time, it is very difficult almost impossible if the information is dispersed across different resources. Therefore, in this case, the Security Information and Event Management (SIEM) system should be used for storing and processing raw data.

II. References.

1. Splunk Fundamentals. . Bushfire resources: https://www.splunk.com.

2. Nessus professional. Retrieved from https://www.tenable.com./products/nessus/nessus-professional

Web: www.promoteukraine.org
Contact: info@promoteukraine.org

Promote Ukraine is a non-profit start-up. It is a politically and governmentally independent organization situated in Belgium. It consists of a thriving team of professionals who on pro bono basis seek to give voice to Ukrainian civil society in Europe and, in particular, throughout Belgium. We believe in European values such as civil rights, good governance and equal opportunities. Through connecting EU businesses and politicians with Ukrainian stakeholders, we facilitate the sharing of best practices between EU and Ukrainian partners with the goal to bring Ukraine closer to EU norms and values from a bottom-up perspective.

promoteukraine
promoteukraine
promoteukraine