Monitoring of department network – administrator view

Ing. Július Baráth, PhD.

Department of informatics, Armed Forces Academy, Liptovský Mikuláš, Slovakia, julius.barath@aos.sk

Abstract. IT infrastructure primary consists of end devices, communication links and networking devices and all of them are prone to misconfiguration errors and vulnerable to attacks. To prevent poor performance, instability of the systems used and to fight with attackers – effective monitoring is a part of everyday admin's duties. The paper answers basic questions: how to collect, normalize and process log and audit information; what is essential information to log across the platforms used; and how to monitor network attached devices in department's network. Collected and filtered data is then indexed with Splunk where data analysis and visualization is made using queries or preconfigured dashboards. Only when full understanding of problem is achieved, proper reaction to fix the problem can be taken. A simple example is provided to better illustrate the process of finding and fixing misconfiguration problem.

Keywords: Splunk, monitoring, audit, network infrastructure

Introduction

Proper, timely, and effective reaction to misuse of IT resources and data thefts requires overall situational awareness and the correct information in the right place at the right time including historical logs. Information acquired from security network devices, operating systems and critical applications on the one side and proper analysis and correct reaction by IT professional on the other side is required to prevent intrusion, data thefts and violation of the security policy. Common, standardized, community and industry accepted protocols for reporting are required to accomplish vision of automated, real time and effective reaction on modern threats.

Both operating system and network/security device vendors provide tools to manipulate generated logs from their products with more or less success to import logs from other party products. Such approach usually ends with multiple and overlapping platforms for monitoring, inconsistencies in logs coverage and difficult manageability. Network and system admins, together with security professionals are asking for one universal, extendable platform for filtering, processing and visualization of logs. One of the products in this category is Splunk. The paper describes how, where and what data to collect and how to use them to answer every day admin questions about functionality and security in department network.

1 Background

ISO 27002 in section Communications and operations management subsection 10.10 Monitoring states that "Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified. An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities. System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model." (1).

To accomplish the idea administrator should:

- configure audit logs to support future investigations and access control monitoring,
- monitor system use (authorized access, privileged operations, unauthorized access attempts, system alerts or failures, changes to, or attempts to change, system security settings and controls),
- protect logging facilities and log information against tampering and unauthorized access,
- log system administrator and system operator activities,
- log and take appropriate action on faults,
- guarantee that the clocks of all relevant information processing systems within an organization or security domain are synchronized with an agreed accurate time source (1).

Many "Best practices for network monitoring" exists and are available[1] [2], some of them put accent on effectiveness and proactive approach using offsite applications, monitoring of both performance and availability of resources, providing of several different notification options, providing application specific alerts and reporting, providing hardware specific alerts or for example have robust reporting capabilities.

The question is how to properly size those capabilities, unify log formats coming from multiple environments, select software for analysis and reporting etc. In the next section we will discuss our approach to monitoring department network.

2 Department network and monitoring

The department oriented to IT research and education uses variety of server and desktop operating systems and applications, network infrastructure, peripherals and security devices (Figure 1).

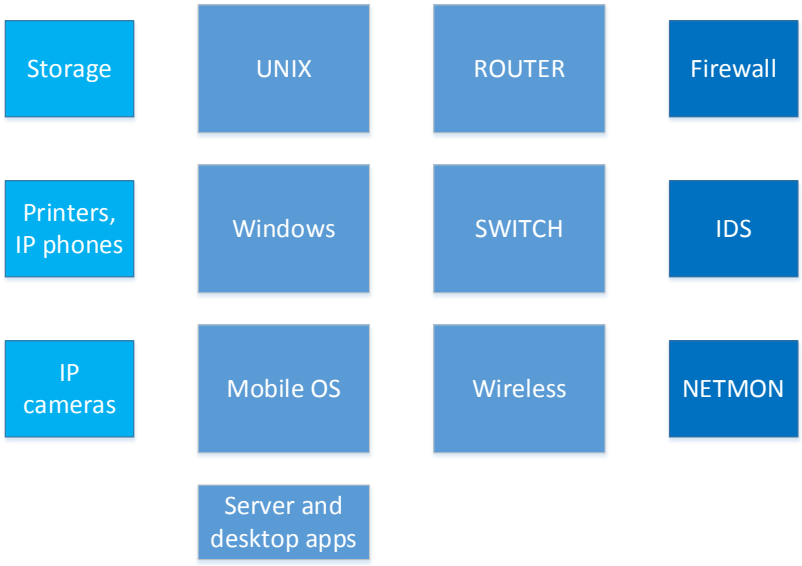

Figure 1 Structure of resources used by department.

Any part of the infrastructure is potential target of attack, misconfigured or vulnerable due software bugs not yet discovered and patched.

Based on number of used devices, the primary target of attacks and misuses are desktop and server operating systems. Basic installation of MS Windows desktop operating system does not provide sufficient log and audit information and to fix it - group security policy should be used to force domain workstations to apply them. Moreover, workstations use antivirus software with its own reporting capabilities and formats.

Question 1: What is essential information to log from workstations?

Problem 1: Logs are stored locally and in specific format.

Server (UNIX and MS Windows) operating systems have extended complexity of logging and auditing because of server applications with specific needs:

- web, mail, database servers,
- network services – DNS, DHCP, Active Directory, web applications,
- special services - Certification Authority, time service, Licensing servers …
- shared applications – licensed development products and more.

Both UNIX and MS Windows servers need to enforce security and configure logging and auditing specific to their configuration. Managing consistent security policy across all servers can be difficult. Problem 1 applies here too.

Question 2: What is essential information to log from servers and their applications?

Second possible target of attacks are network attached devices – some of them are disk storages, network printers, IP phones, IP video cameras, remotely operated door locks and more. Those devices have in most cases old firmware versions and limited or missing logging features.

Question 3: How to monitor network attached devices?

[1] http://www.pcworld.com/article/144635/guide_network_management_monitoring.html
[2] http://lanlogic.com/pdf/Lanlogic-Network-Monitoring-Best-Practices.pdf

Third possible target of attacks are network infrastructure devices and monitoring devices. Routers, switches, firewalls, IDS and network monitors (if purchased as managed devices) have specialized operating systems and usually good logging capabilities. As any other hardware with an operating system, it has to be secured, patched and remote logging should be configured.

Question 4: What is essential information to log from network infrastructure and monitoring devices?

To generalize, we should answer following questions:

- how to collect, normalize and process log and audit information,
- what is essential information to log across the platforms used,
- how to monitor network attached devices.

2.1 How to collect, normalize and process log and audit information?

To collect process and present data the Splunk[3] software was chosen. "Splunk is the engine for machine data. Splunk can read data from just about any source imaginable, including student registration systems, learning management systems, networks, web servers, remote sensors, mobile and online learning applications, legacy applications, application servers and structured databases. By centralizing all this data into a single console, Splunk provides unparalleled insight into problems, usage patterns and trends across an entire campus IT infrastructure. In addition, institutional usage is not limited by the number of machines, data sources, or users—it is only limited by the total data volume that is indexed. This gives IT the ability to control utilization without being locked into a per-user or per-machine fee" (3).

Data collection and processing can be described using Figure 2. As a prerequisite to collect useful data, all devices have synchronized time and are managed by local network administrator. **Desktops** and **servers** are able to collect logs and audit information locally and send it to Splunk – Option 1 Figure 2, but on the Splunk side we have to filter less significant events and we are losing some logs specific for application servers or network services (to name some DHCP logs for MS Windows server are stored in log files and not central event log system, SharePoint server produces logs differently too etc). Specialized Splunk client lite (with server/platform specific extensions) can be remotely installed on critical servers and configuration file allows select/filter what information is send, where it should be processed and provides identification of source. Information send includes health, resource utilization, updates, security, change management and more.

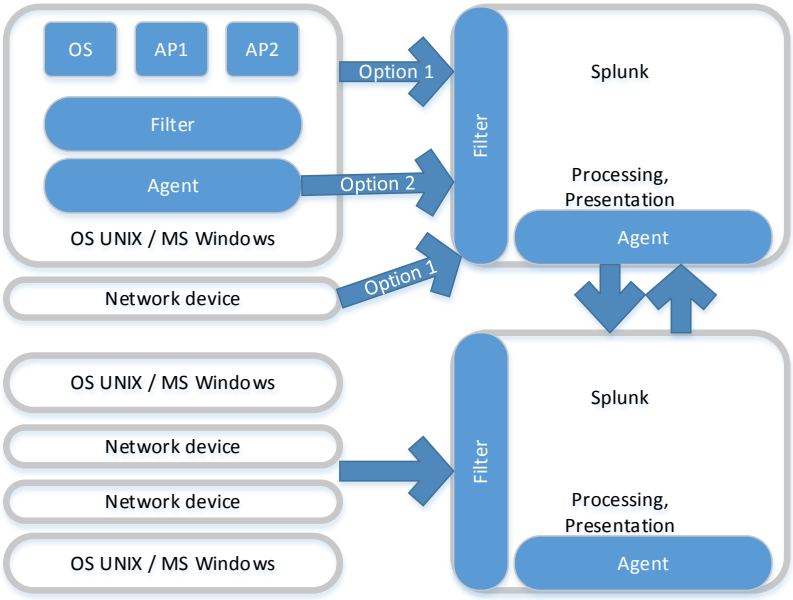

Figure 2 Data collection and processing.

Network and **security devices** (routers, switches, IDS, firewall) manufactured by Cisco systems are remotely manageable devices with appropriate log capabilities. Logs from these devices are send directly to Splunk and no extra effort is needed to interpret them (thanks to plugins created and maintained by the company). Basic logging configuration for router usually includes setting for timestamps, logging level and logging syslog server.

[3] http://www.splunk.com/

More advanced monitoring options are change auditing, smart call home logging, interface monitor changes, DHCP utilization logging, ACL logging or for switches - MAC move notifications, STP logging, IP SLA logging etc. A short example of advanced monitoring configurations follows.

```
Advanced logging includes change auditing:
archive
 log config
  logging enable
  logging size 200
  notify syslog contenttype plaintext
  hidekeys
!
login on-failure log
login on-success log
logging userinfo
!
```

```
Smart call home logging includes:
ip http client source-interface FastEthernet 0/0
!
service call-home
call-home
 contact-email-addr xy@aos.sk
 site-id "kti"
 profile "Splunk"
  destination transport-method http
  destination address http http://XX.XX.XX.XX:YYYY
  subscribe-to-alert-group diagnostic severity debug
  subscribe-to-alert-group environment severity debug
  subscribe-to-alert-group inventory
  subscribe-to-alert-group inventory periodic daily 20:00
!
```

2.2 How to monitor network attached devices?

This category of devices has specific needs, because not all of them support direct open interface to access logs. If attached device is monitored by server or host based application, Splunk client lite can be used to access logs. In other cases only L2-L7 communication monitoring can be used (via specialized probe or monitor).

To monitor special communication channels like Locked-down VDI monitoring (printer and USB channels) see ExtraHop for Security and Compliance[4]. The ExtraHop platform analyzes wire data, which is all L2-L7 communications between systems including full bi-directional transaction payloads.

2.3 What is essential information to log across the platforms used?

General guidance for logging is provided by (1) where it is written that “Audit logs should include, when relevant:

a) user IDs,
b) dates, times, and details of key events, e.g. log-on and log-off,
c) terminal identity or location if possible,
d) records of successful and rejected system access attempts,
e) records of successful and rejected data and other resource access attempts,
f) changes to system configuration,
g) use of privileges,
h) use of system utilities and applications,

[4] https://splunkbase.splunk.com/app/1757/

i) files accessed and the kind of access,
j) network addresses and protocols,
k) alarms raised by the access control system,
l) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems."

And monitoring system should record:
a) authorized access,
b) all privileged operations,
c) unauthorized access attempts,
d) system alerts or failures,
e) changes to, or attempts to change, system security settings and controls.

How often the results of monitoring activities are reviewed should depend on the risks involved. Risk factors that should be considered include the:
a) criticality of the application processes,
b) value, sensitivity, and criticality of the information involved,
c) past experience of system infiltration and misuse, and the frequency of vulnerabilities being exploited,
d) extent of system interconnection (particularly public networks),
e) logging facility being de-activated (1).

For MS windows server it is easy to generate hundreds of thousands records per day per server and deeper understanding of system is required to define audit and logging and to filter unwanted logs (4, 5, 7-9). For UNIX systems you can generate periodic logs using system utilities (sar, tcpdump, iostat, mpstat, IP Traf etc) and then use them to extend Slunk Universal Forwarder for Linux capabilities or Linux Auditd[5] app capabilities. To route and filter data on Splunk installations see (2).

3 Presenting data with Splunk

Once textual data (from switches, routers, firewalls, desktops, servers, web servers, databases, network services) is indexed by Splunk, it is analyzed by system and network admins or security experts to find anomalies, configuration errors and all sorts of breaches using Splunk's Search Processing Language.

As you use Splunk to answer questions, you'll find that you can break the task into three phases.

1. First, identify the data that can answer your question.
2. Second, transform the data into the results that can answer your question.
3. Third, display the answer in a report, interactive chart, or graph to make it intelligible to a wide range of audiences (6).

Nice thing about Splunk is that your findings may vary from the most common to the most unusual ones. Results can be summarized via statistics or represent accidents as group of events, providing necessary level of operational intelligence.

To find the needle in the haystack we use search app. Search lets you create search query, change time range, run query, refine search, save search and more. An alternative to type search commands is to use dashboards, followed by detail inspection of problems.

[5] https://splunkbase.splunk.com/app/2642/

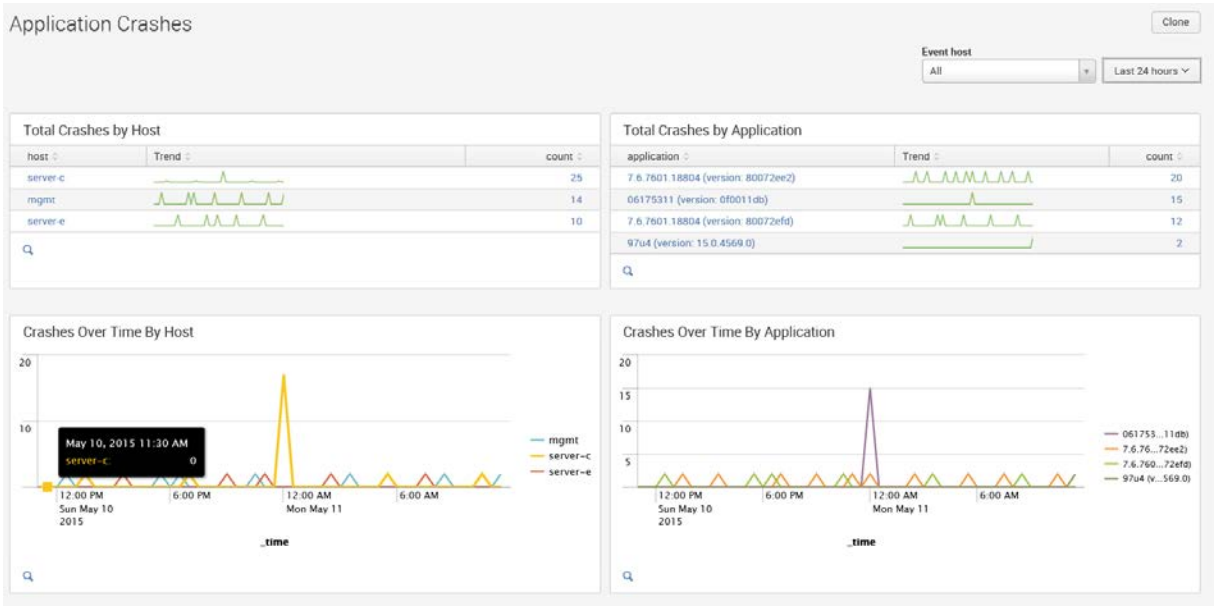

Figure 3 Application crashes dashboard.

Figure 3 shows 25 crashes for server-c in last 24 hours, using references in crashes by application the reason of problems is determined, inspected in detail view using preconfigured search query

```
eventtype="wineventlog_windows" EventCode="1001" Event_Name="*" host="*"
| eval application=P1." (version: ".P2.")" | search applica-
tion="7.6.7601.18804 (version: 80072ee2)"
```

Based on a detail view (not shown in the paper) we can quickly conclude that problem comes from windows update service misconfiguration. After fixing the problem you will not see such entries for server-c any more.

Dashboards are usually part of specifically created apps from different vendors like Microsoft, Cisco etc. and if needed you can create your own. It is very useful to create your own queries, transform them to events and run them automatically to detect possible configuration problems or violation to security policy. Such approach automatizes routine actions and customizes working environment.

4 Conclusion

Working with Splunk consists of gathering data, transferring them into answers and visualizing of review data to get answers. During the experimentation phase more than 66 million records from servers and routers were analyzed, many lesser and greater misconfigurations were fixed and a few security violation accidents were found. As any other technology on the market, when properly used by a trained professional, Splunk can help to understand problems in your information infrastructure. It will not fix the problem; you must take proper actions to fix them. If you will not regularly review collected data and actively search for new forms of attacks, your IT infrastructure and processed data will not be safe.

References

1. ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls. In. Switzerland: International Organization for Standardization.
2. Route and filter data [online]. [cited may 2015]. Available from:<http://docs.splunk.com/Documentation/Splunk/6.2.2/Forwarding/Routeandfilterdatad>.
3. Splunk for Higher Education and Universities [online]. [cited june 10 2014]. Available from:<http://www.splunk.com/web_assets/pdfs/secure/Splunk_for_Higher_Education.pdf>.
4. Planning and Deploying Advanced Security Audit Policies [online]. 2009 2015]. Available from:<https://technet.microsoft.com/en-us/library/ee513968(v=ws.10).aspx>.
5. (T) Filtering or trimming Windows logs the right way, NOT by Event ID [online]. 2014 [cited may 2015]. Available from:<http://hackerhurricane.blogspot.sk/2014/07/t-filtering-or-trimming-windows-logs.html>.

6. CARASSO, D. Exploring Splunk [online]. CITO Research, 2012. Available from World Wide Web:<http://www.splunk.com/goto/book>.
7. MELBER, D. *Windows group policy resource kit : Windows server 2008 and Windows vista*. Edtion ed. Redmond, WA: Microsoft Press, 2008. xxiv, 511 p. p. ISBN 9780735625143 (perfect bound).
8. Security Log Step-by-Step: Avoiding Audit Policy Configuration Pitfalls [online]. 2012 [cited may 2015]. Available from:<https://www.ultimatewindowssecurity.com/blog/default.aspx?p=aa6c16dc-8bb8-40e3-aac9-d2c7eaa6c5f6>.
9. TULLOCH, M. *Introducing Windows Server 2012 R2*. Edtion ed. Redmond, Washington: Microsoft, 2013. xi, 227 pages p. ISBN 9780735682788 (pbk.) 073568278X (pbk.).