Top 100 Linux Log Events for Security Monitoring in a SOC

https://www.linkedin.com/in/jbassim/

🌟 **Support me and follow my LinkedIn profile for more insights and updates!** Thanks for your support. 🚀

Top 100 Linux Log Events for Security Monitoring in a SOC

Event ID	Source	Description	Log File	Severity Level	Potential Security Indicator
1001	`auth`	Successful login.	`/var/log/auth.log`	Informational	Valid user logins
1002	`auth`	Successful logout.	`/var/log/auth.log`	Informational	Normal user logout
2001	`auth`	Failed login attempt.	`/var/log/auth.log`	Warning	Brute force attacks, unauthorized access attempts
2002	`auth`	User account locked due to multiple failed login attempts.	`/var/log/auth.log`	Critical	Possible brute force attacks
3001	`kern`	Critical kernel error message.	`/var/log/kern.log, dmesg`	Error	System failures, critical issues
3002	`kern`	Kernel warning about low resources.	`/var/log/kern.log, dmesg`	Warning	Resource shortages impacting system stability
4001	`syslog`	General system message.	`/var/log/syslog`	Informational	Informational about system status
4002	`syslog`	System configuration change event.	`/var/log/syslog`	Warning	Unauthorized configuration changes
5001	`auditd`	Access to sensitive file.	`/var/log/audit/audit.log`	Critical	Unauthorized access to sensitive files
5002	`auditd`	Modification of a critical file.	`/var/log/audit/audit.log`	Critical	Unauthorized file modifications
6001	`daemon`	Service start or stop event.	`/var/log/daemon.log`	Informational	Service status changes
6002	`daemon`	Service error event.	`/var/log/daemon.log`	Error	Service failures impacting security
7001	`selinux`	SELinux policy violation.	`/var/log/audit/audit.log`	Critical	SELinux policy violations
7002	`selinux`	SELinux denied access due to policy.	`/var/log/audit/audit.log`	Warning	Access attempts blocked by SELinux

Event ID	Source	Description	Log File	Severity Level	Potential Security Indicator
8001	`crond`	Cron job execution event.	`/var/log/cron`	Informational	Scheduled tasks execution
8002	`crond`	Cron job execution error.	`/var/log/cron`	Error	Issues with scheduled tasks
9001	`ssh`	SSH login success.	`/var/log/auth.log`	Informational	Successful remote access
9002	`ssh`	SSH login failure.	`/var/log/auth.log`	Warning	Unauthorized remote access attempts
10001	`syslog`	System boot event.	`/var/log/syslog`	Informational	System startups and restarts
10002	`syslog`	System shutdown event.	`/var/log/syslog`	Informational	Unexpected shutdowns or restarts
11001	`auditd`	Execution of a privileged command.	`/var/log/audit/audit.log`	Critical	Privilege escalation attempts
11002	`auditd`	Attempt to access unauthorized resource.	`/var/log/audit/audit.log`	Critical	Attempts to access restricted resources
12001	`daemon`	Application crash event.	`/var/log/daemon.log`	Error	Application crashes
12002	`daemon`	Service configuration change.	`/var/log/daemon.log`	Warning	Unauthorized changes in service configurations
13001	`kern`	System memory error.	`/var/log/kern.log`, `dmesg`	Error	Memory issues or failures
13002	`kern`	CPU error or issue.	`/var/log/kern.log`, `dmesg`	Error	CPU-related problems
14001	`auth`	Password change event.	`/var/log/auth.log`	Informational	Password changes by users
14002	`auth`	Failed password change attempt.	`/var/log/auth.log`	Warning	Failed attempts to change passwords
15001	`syslog`	Disk space warning.	`/var/log/syslog`	Warning	Low disk space issues
15002	`syslog`	Disk space critical.	`/var/log/syslog`	Critical	Critical low disk space
16001	`auditd`	User privilege escalation.	`/var/log/audit/audit.log`	Critical	Unauthorized privilege escalation
16002	`auditd`	Audit policy change.	`/var/log/audit/audit.log`	Warning	Changes to audit policies

Event ID	Source	Description	Log File	Severity Level	Potential Security Indicator
17001	syslog	System load average warning.	/var/log/syslog	Warning	High system load conditions
17002	syslog	System load average critical.	/var/log/syslog	Critical	Critical system load conditions
18001	auditd	File access denied due to permissions.	/var/log/audit/audit.log	Warning	Permission issues on file access
18002	auditd	Unauthorized file modification detected.	/var/log/audit/audit.log	Critical	Unauthorized changes to files
19001	syslog	Network interface up event.	/var/log/syslog	Informational	Changes in network interface status
19002	syslog	Network interface down event.	/var/log/syslog	Warning	Unexpected network interface failures
20001	daemon	Service start or stop from a specific user.	/var/log/daemon.log	Informational	Service actions by users
20002	daemon	Service configuration change by a specific user.	/var/log/daemon.log	Warning	Unauthorized changes in service configurations
21001	kern	Hardware error detected.	/var/log/kern.log, dmesg	Critical	Hardware failures or issues
21002	kern	Filesystem error.	/var/log/kern.log, dmesg	Error	Filesystem issues and corruption
22001	auth	Suspicious authentication attempts.	/var/log/auth.log	Critical	Potential brute force or unauthorized access
22002	auth	Repeated failed login attempts.	/var/log/auth.log	Warning	Multiple failed login attempts
23001	auditd	Unauthorized access to a network resource.	/var/log/audit/audit.log	Critical	Unauthorized network access attempts
23002	auditd	Network configuration changes.	/var/log/audit/audit.log	Warning	Unauthorized network configuration changes
24001	syslog	Application error logs.	/var/log/syslog	Error	Application errors impacting system security
24002	syslog	Application warning logs.	/var/log/syslog	Warning	Application warnings that may indicate issues
25001	kern	Unusual kernel messages or events.	/var/log/kern.log,	Warning	Unusual system behavior or anomalies

Event ID	Source	Description	Log File	Severity Level	Potential Security Indicator
			dmesg		
25002	kern	Critical kernel panic or crash.	/var/log/kern.log, dmesg	Critical	System instability or crashes
26001	auth	User account creation event.	/var/log/auth.log	Informational	New user account creation
26002	auth	User account deletion event.	/var/log/auth.log	Informational	User account deletions
27001	auditd	Successful privilege escalation.	/var/log/audit/audit.log	Critical	Elevated privileges granted
27002	auditd	Failed privilege escalation attempt.	/var/log/audit/audit.log	Warning	Failed attempts to gain elevated privileges
28001	syslog	Software update event.	/var/log/syslog	Informational	Software updates and patches
28002	syslog	Software update failure.	/var/log/syslog	Error	Issues with software updates
29001	kern	System clock changes.	/var/log/kern.log, dmesg	Informational	Changes to system time
29002	kern	NTP synchronization issues.	/var/log/kern.log, dmesg	Warning	Issues with network time protocol synchronization
30001	auth	User password expiration warning.	/var/log/auth.log	Warning	Passwords nearing expiration
30002	auth	User password change due to expiration.	/var/log/auth.log	Informational	Password changes due to expiration
31001	syslog	Network traffic spikes detected.	/var/log/syslog	Warning	Unusual network activity
31002	syslog	Network interface errors.	/var/log/syslog	Error	Network connectivity issues
32001	auditd	User session timeout event.	/var/log/audit/audit.log	Informational	User session timeouts
32002	auditd	Suspicious user activity detected.	/var/log/audit/audit.log	Warning	Potentially malicious user actions
33001	syslog	System reboot initiated.	/var/log/syslog	Informational	System restarts
33002	syslog	System shutdown initiated.	/var/log/syslog	Informational	System shutdowns
34001	kern	Disk I/O errors.	/var/log/	Error	Disk read/write issues

Event ID	Source	Description	Log File	Severity Level	Potential Security Indicator
			`kern.log, dmesg`		
34002	`kern`	Disk partition changes.	`/var/log/kern.log, dmesg`	Warning	Unauthorized disk partition modifications
35001	`auth`	Account expiration warning.	`/var/log/auth.log`	Warning	User account expiration warnings
35002	`auth`	Account expiration event.	`/var/log/auth.log`	Informational	User account expirations
36001	`auditd`	Unauthorized changes to system configurations.	`/var/log/audit/audit.log`	Critical	Critical configuration changes
36002	`auditd`	Unauthorized changes to application configurations.	`/var/log/audit/audit.log`	Warning	Changes to application settings
37001	`syslog`	Security policy updates.	`/var/log/syslog`	Informational	Updates to security policies
37002	`syslog`	Security policy violations.	`/var/log/syslog`	Warning	Violations of security policies
38001	`kern`	Hardware temperature warnings.	`/var/log/kern.log, dmesg`	Warning	Overheating issues
38002	`kern`	Hardware failure events.	`/var/log/kern.log, dmesg`	Critical	Hardware failures impacting system stability
39001	`auditd`	Suspicious command execution detected.	`/var/log/audit/audit.log`	Critical	Potentially malicious command executions
39002	`auditd`	Unauthorized command execution detected.	`/var/log/audit/audit.log`	Warning	Commands executed without proper authorization
40001	`syslog`	Service status change event.	`/var/log/syslog`	Informational	Changes in the status of system services
40002	`syslog`	Unexpected service termination.	`/var/log/syslog`	Error	Unexpected service terminations
41001	`daemon`	Daemon error messages.	`/var/log/daemon.log`	Error	Errors in daemon services
41002	`daemon`	Daemon warnings.	`/var/log/daemon.log`	Warning	Warnings in daemon services
42001	`auditd`	Sensitive data access detected.	`/var/log/audit/audit.log`	Critical	Unauthorized access to sensitive data
42002	`auditd`	Changes to sensitive	`/var/log/`	Critical	Unauthorized changes

Event ID	Source	Description	Log File	Severity Level	Potential Security Indicator
		data.	audit/audit.log		to sensitive data
43001	syslog	Critical system updates applied.	/var/log/syslog	Informational	System updates that could affect security
43002	syslog	System update failures.	/var/log/syslog	Error	Issues with applying system updates
44001	auth	Unauthorized user privilege escalation attempt.	/var/log/auth.log	Critical	Privilege escalation attempts
44002	auth	Privilege escalation success event.	/var/log/auth.log	Critical	Successful unauthorized privilege escalation
45001	kern	System call violations detected.	/var/log/kern.log, dmesg	Warning	Unauthorized system calls
45002	kern	Unauthorized kernel module loaded.	/var/log/kern.log, dmesg	Critical	Loading of unauthorized kernel modules
46001	auditd	File system access issues.	/var/log/audit/audit.log	Error	Issues with file system access
46002	auditd	Unauthorized file deletions.	/var/log/audit/audit.log	Critical	Unauthorized deletions of important files
47001	syslog	User account changes detected.	/var/log/syslog	Informational	Creation, modification, or deletion of user accounts
47002	syslog	Critical user account changes.	/var/log/syslog	Warning	Significant changes to user accounts
48001	auditd	Access to protected resources.	/var/log/audit/audit.log	Warning	Unauthorized access to protected resources
48002	auditd	Unauthorized attempts to modify protected resources.	/var/log/audit/audit.log	Critical	Critical modifications to protected resources
49001	syslog	Network configuration changes.	/var/log/syslog	Warning	Changes to network configurations
49002	syslog	Unauthorized network configuration changes.	/var/log/syslog	Critical	Unauthorized changes to network settings

https://www.linkedin.com/in/jbassim/

🌟 **Support me and follow my LinkedIn profile for more insights and updates!** Thanks for your support. 🚀