# ANALYZE **THIS**

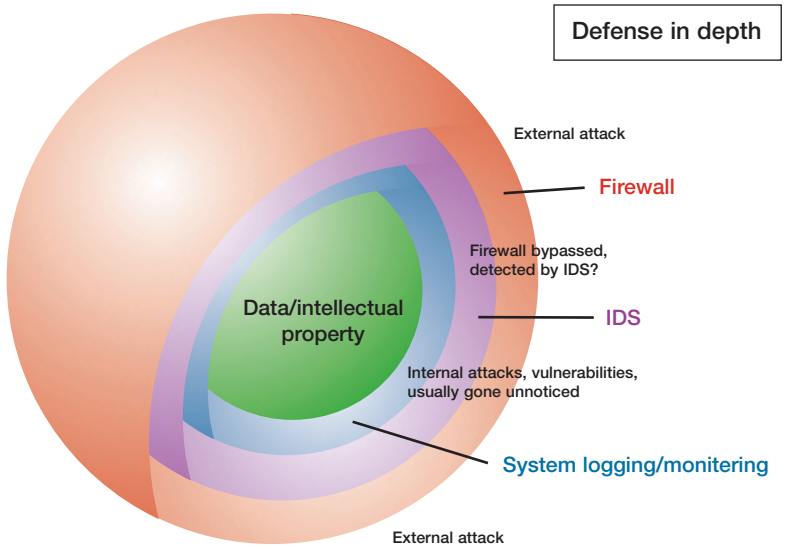
SYSTEM LOGGING AND UTILIZATION REPORTING CAN HELP IMPROVE COMPUTER SYSTEM AND NETWORK SECURITY, SAYS HARAL TSITSIVAS.

Good system and network security starts with a good understanding of an organization's operating environment. Organizations that have a good understanding of their operating environment – and that environment's limitations and vulnerabilities – should be able to secure their system relatively easily. Maintaining a high level of system security, however, is an on-going process that requires continued vigilance and solid organizational policies and procedures. Pro-active system administrators not only keep their systems patched, but also continuously monitor system and network logs and system resource usage reports for interesting events.

All systems can log interesting system events, although sometimes the event types and depth of logging information can vary from system to system. On UNIX systems, for example, there are several facilities that could generate messages using the syslog facility. The information collected by syslog is a valuable resource in determining the health of the system, and when reviewed regularly can provide an advance warning for some types of attacks.

On Windows systems, the event log can record various types of application and security events that can be useful when analyzing system errors or when tracing possible intrusions or security compromises. Syslog-type software is also available for Windows systems, thus allowing for central reporting of interesting system events across all platforms.

To improve security on UNIX systems, the syslog UDP port (514) should be blocked at the firewall in order to reduce the likelihood of a buffer overflow attack or other vulnerability being remotely exploited, and remote logging should be disabled unless the host acts as a central log server.




Traditionally, resource accounting and chargeback products have been used to track shared resources on central servers, and for utilization reporting on server consolidation projects. Development and production environments that concurrently work on multiple projects using common resources/computers have also been traditional users of chargeback products.

Analysis of system usage data can be very useful in improving system performance by helping detect performance bottlenecks and in the detection of intrusions, since anomalies in chargeback data can sometimes reveal inefficient applications and/or misuse of computer resources. An IT department that finds unusual usage patterns or excessively high usage during review of chargeback records should consult with the user organization to determine whether an inefficient application can be improved. This would reduce its resource utilization in order to save money for the user organization, and spare the IT organization from planning for a system upgrade to meet bogus system demands. Likewise, a spike in user activity, or worse, a spike in activity of previously dormant accounts and projects may indicate that security has been compromised or that the systems are misused.

On UNIX systems, the standard system accounting files can provide a wealth of system usage information when analyzed on a regular basis, and can be used for both chargeback and capacity planning purposes. 'Wtmp' or 'wtmpx' and 'pacct' are the standard UNIX system accounting files, containing login information and resource usage information by processes respectively. The 'last' and 'acctcom' programs can be used to view detailed usage data while the 'acctcon' and 'acctprc'/'acctcms' programs can be used to view summarized data.

Windows systems can record login, logout, application start and application stop events, although resource usage information is not recorded in the event log. This type of auditing, however, is turned off by default – so these changes should be applied site-wide through the group or enterprise audit policy by turning on auditing of logon and logoff events and process tracking events. The 'dumpel' utility, available on the Resource Kit, can be used to report on the various event logs or to format event log entries for export to spreadsheets (or other applications) for further review.

Commercial products can simplify the presentation of system usage data for chargeback. UNISOL JobAcct from UniSolutions Associates, for example, can generate system usage reports by user, group, project or cost-center, for one or more computers on the network, collecting the same type of data on both Windows and UNIX systems. JobAcct can collect application resource usage information on Windows systems without relying on the limited data available through the event log, thus providing a consistent report across various operating system types.

There are several free scripts and tools available on the web for UNIX systems that can be used by system administrators to summarize and monitor the syslog and login accounting files. One syslog summary tool is newlogcheck, which enhances security by reducing the amount of log entries administrators have to examine, and categorizing the log entries. Sentryd is a Perl script that monitors the syslog and wtmp files for unusual events and bad login attempts, and notifies users (by broadcast) of selected events.

There are also tools for more specialized log analysis that can parse log entries in real time and correlate system and network events, such as SEC (the Simple Event Correlation tool), Swatch, Logsurfer, and Logwatch. Several vendors also provide managed security (e.g. analyzing firewall data recorded in syslog files), while several vendors provide managed security services typically including firewall log analysis, intrusion detection, virus protection, gateway services, and vulnerability assessment and policy compliance services.

**"Analysis of system usage data can be very useful in improving system performance by helping detect performance bottlenecks and in the detection of intrusions"**

Organizations considering outsourcing certain security services should consult the paper Outsourcing Managed Security Services from CERT in order to better understand the benefits and risks involved with hiring a Managed Security Service Provider (MSSP) and getting maximum value for their security budget without compromising system security – or giving up too much control of their IT environment.

Finally, checking for login errors should also be performed regularly, perhaps by incorporating the process together with an automated syslog analysis procedure. The location of the logged login errors differs from machine to machine, but all systems log some type of login errors. When auditing is turned on for logon success and failures on Windows, the Security event log will contain these events.

Pulling together all of the logs and analyzing them regularly (preferably in an automated process) is the first step in establishing an incident response policy. An automated log analysis process that notifies administrative personnel promptly can be an invaluable tool to providing a quick response to system attacks or other significant security events, that can stop a security breach early enough before irreparable damage can take place.

## CONCLUSION

Maintaining secure systems and networks is an ongoing process fraught with difficulties, which are further exacerbated in heterogeneous, multi-Operating System environments by the multitude of differences between the various operating systems and the procedures that must be followed in order to maintain a high level of system and network security.

To keep systems and networks secure, an organization must adapt the defense-in-depth mindset and work on as many security layers as possible, from the external facing firewalls to the internal development servers. Firewalls are an essential first line of defense and IDS systems are successful in tracking and preventing some types of internal threats or attacks that have penetrated the firewall. However, organizations that consistently analyze, report, and use the collected system utilization data and logged interesting events can respond quicker to security threats and thus avoid or minimize the damage of these threats. ■

Haral Tsitsivas is a GIAC GSEC certified Information Security Professional and is the president of UniSolutions Associates, providing system and network security consulting services, and delivering system resource accounting and chargeback solutions and unattended network backup software. He holds Bachelors and Masters of Science degrees from California State University, Northridge and a Masters of Business Administration degree from Pepperdine University, Malibu, California.