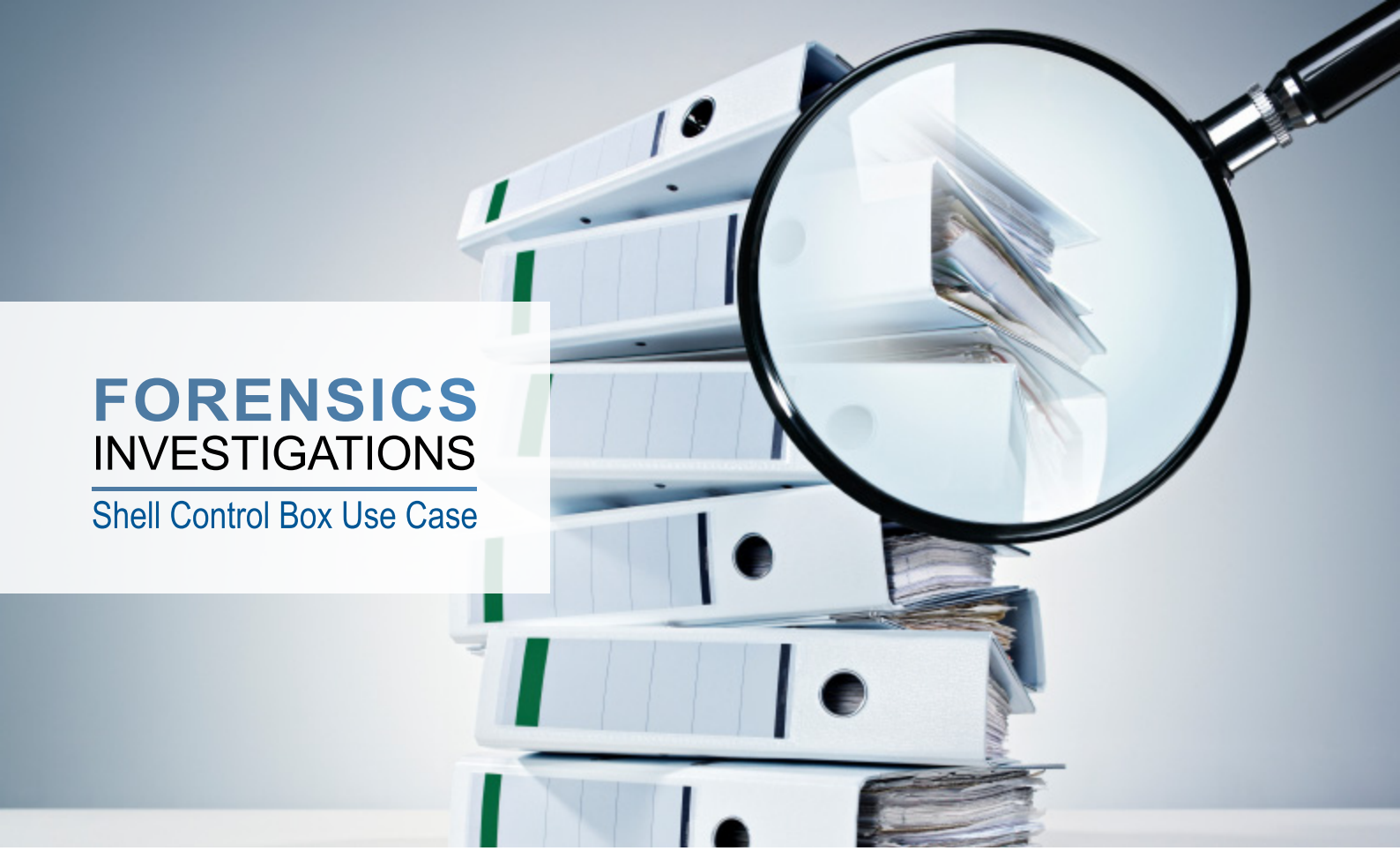

FORENSICS INVESTIGATIONS

Shell Control Box Use Case

The Challenge - “Who did what on servers?”

The simple question “Who accessed our server and what did he or she do?” is one of the toughest questions to answer in IT today. System management tools are improving companies’ ability to handle system error, but the solution to human error, the number one cause for server downtime, remains elusive. System administrators have privileged access and can manage the whole IT environment without strict control. Consequently, companies can only hope that these super-users are trustworthy. In many cases, computer forensics by larger companies is performed by local Computer Emergency Response (CERT) or Computer Incident Response Teams (CIRT). However, without the reliable recording of administrative access to the servers, the investigation of incidents becomes expensive and circumstantial.

In addition, external standards such as the ISO 2700x or the PCI-DSS specify strict measures to support future investigations, by requiring the recording of user activities or fault logging in place.

Without user session recording the question of who did what and when is almost impossible to answer, and often leads to accusations along with the time and money wasted on investigating the incident. To avoid this, a tamper-proof session recording solution could be implemented.

Key Shell Control Box benefits for forensics

- audit SSH, RDP, VNC, Citrix ICA, Telnet and other protocols
- search and re-play audit trails for quick forensics
- free-text search in audit trail content
- tamper-proof audit trails for privacy and compliance
- record raw data and export to pcap-format
- SCP/SFTP file transfer analysis

The Solution - Tamper-proof Activity Recording

BalaBit Shell Control Box (SCB) is a cost-efficient and compliant solution to aid in the investigation of incidents related to servers. For example, in case of an unexpected shutdown, data leakage, or database manipulation, the circumstances of the event are readily available in audit trails so the cause of the incident can be quickly identified. The recorded audit trails can be played back like a movie – recreating all actions of the administrator. Consequently, SCB helps to find not only the root cause of a problem, but also the responsible person. This is especially important in case of business-critical servers, or if the company has outsourced its server administration to an external company.

Audit trails are invaluable for both real-time and post-event investigations. They enable the internal auditor to search, for example, for all the users who accessed a specific account number in a specific time-frame across any platform in the enterprise. As audit trail content can be easily interpreted, SCB eliminates the need for costly external consultants in the case of forensics investigations.

SCB prevents anyone from modifying the audited information as audit trails are time stamped, encrypted, and signed. This makes SCB capable of reconstructing events and providing tamper-proof evidence in case of legal proceedings, too.

Technical Implementation

SCB is an independent network device that operates transparently, and extracts audit information directly from the communication between the client and the server. Audit trails can be browsed online, or viewed real-time to monitor the activities of the administrators. The Audit Player enables fast forwarding during replays, as well as free-text search for events making forensics investigations quick and cost-efficient. By free-text search capability the alphanumeric commands entered by the user or displayed texts in graphical protocols (e.g. RDP) can also be searchable. It is also possible to execute searches on a large number of audit trails to find sessions that contain a specific information or event.

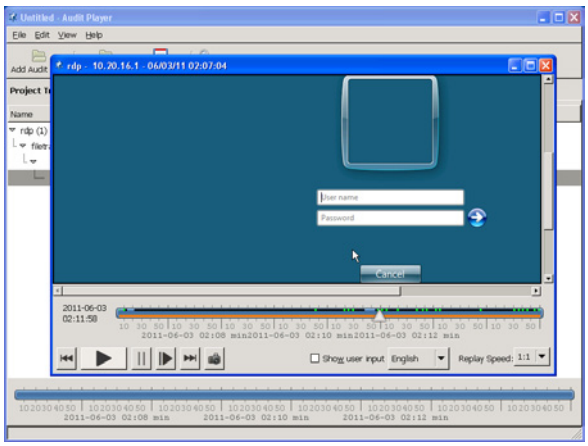

Figure 1. Replaying an audit trail

In addition to recording audit trails of the inspected protocols, embedded protocols (for example, other protocols tunneled in SSH, port-forwarding) and transferred files can be recorded as well. Recorded files from SCP and SFTP connections can be extracted for further analysis. It is even possible to convert the audited traffic into packet capture (pcap) format to analyze it with external tools.

For example, if a service becomes unavailable, you can get a list of users who recently accessed the server, check the type of their access (file transfer, shell, etc.) to find which might affect the service, check the content of transferred files, get a list of commands typed or replay the suspicious sessions.

About BalaBit

BalaBit IT Security is an innovative information security company, one of the global leaders in developing privileged activity monitoring, trusted logging and proxy-based gateway technologies to help customers be protected against insider and outsider threats and meet security and compliance regulations. BalaBit, the second fastest-growing IT Security company in the Central European region concerning Deloitte Technology Fast 50 list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Its R&D and global support centers are located in Hungary, Europe.

More information: www.balabit.com

Learn More

- Shell Control Box homepage
- PCI and ISO27001 compliance and forensics in auditing remote server access
- Request an evaluation version
- Request a callback