| | | | EVENT_OPEN | |
|---|------------------------------|-------------------------|-----------------------|---|
| | | | EVENT_OPEN | {'file': '/dev/kmem'}3 |
| | EVENT_RECVFROM | {'subject': 'sshd'}6 | EVENT_EXECUTE | {'file': '/usr/local/sbin/lsof'}3 |
| | EVENT_SENDTO | (subject: sale) o | EVENT_CLOSE | |
| | EVENT_RECVFROM | | | {'file': '/var/mail/henry.lock'}3 |
| | | {'subject': 'smtpd'}4 | EVENT_CLOSE | |
| | EVENT_SENDTO | | EVENT_OPEN | {'file': '/etc/resolv.conf'} 3 |
| | EVENT_RECVFROM | {'subject': 'links'}11 | EVENT_CLOSE | |
| {'netflow': '128.55.12.10:53'}3 | EVENT_SENDTO | | EVENT_CLOSE | |
| (Model V 12 de la 12 | EVENT_RECVFROM EVENT_SENDTO | {'subject': 'lsof'}3 | EVENT_OPEN | |
| | | | EVENT_CLOSE | |
| | | {'subject': 'local'}4 | EVENT_OPEN EVENT_OPEN | {'file': '/etc/services'}3 |
| | | | _ | {'file': '/var/run/ld-elf.so.hints'}2 |
| | EVENT_RECVFROM | | EVENT_CLOSE | |
| | | | EVENT_OPEN | {'file': '/etc/nsswitch.conf'}4 |
| | | | EVENT_OPEN | {'file': '/etc/pwd.db'}7 |
| | | | EVENT_CLOSE | |
| | | | EVENT_OPEN | {'netflow': '128.55.12.166:33800'}3 |
| | | | | {'netflow': '128.55.12.167:42129'}3 |
| | EVENT_CLOSE \ | | EVENT_WRITE | |
| | | | EVENT_WRITE | {'file': '/etc/pam.d/imap'}3 |
| | | | EVENT_OPEN | {'file': '/etc/login.conf'}6 |
| | | | EVENT_OPEN | |
| | | | EVENT_OPEN | {'file': '/usr/share/zoneinfo/posixrules'}4 |
| | | | EVENT_OPEN | {'file': '/etc/pam.d/other'}3 |
| | | | 2,2,1,2,1 | |
| | | | EVENT_WRITE | {'file': '/tmp/.31.29d08'}3 |
| | | | EVENT_WRITE | {'file': '/tmp/.31.29adf}3 |
| | | {'subject': 'imapd'}3 | EVENT_WRITE | {'netflow': '128.55.12.118:46790'}3 |
| | EVENT_RECVFROM | { subject : Illiapu } 3 | EVENT_WRITE | { netnow : 128.33.12.118.40790 } 3 |
| | | | EVENT_WRITE | {'netflow': '128.55.12.118:46791'}3 |
| | | | EVENT_WRITE | {'netflow': '128.55.12.166:56116'}3 |
| | | | | (netnew : 120.33.12.100.30110) 3 |
| | | | EVENT_WRITE | {'netflow': '128.55.12.118:46789'}3 |
| | | | | {'netflow': '128.55.12.166:49245'}3 |
| | | | EVENT_CLOSE | |
| | | | | {'file': '/home/george/.mailboxlist'}3 |
| | | | EVENT_WRITE | {'netflow': '128.55.12.167:42138'}3 |
| | | | EVENT_OPEN | |
| | | | EVENT_OPEN | {'file': '/var/mail/george'}3 |
| | | | | {'file': '/home/george/Sent'}3 |
| | EVENT_SENDTO | | EVENT_CLOSE | |
| | EVENT_SENDIO | | | {'file': '/usr/share/zoneinfo/UTC'}4 |
| | | | EVENT_OPEN | {'file': '/var/mail/bob'}3 |
| | | | EVENT_WRITE | |
| | | | EVENT_OPEN | {'file': '/tmp/.31.29ada'}3 |
| | | | | {'file': '/etc/spwd.db'}6 |
| | | | EVENT_OPEN | |
| | | \ \ \ \ \ \ | EVENT_EXECUTE | {'file': '/usr/local/etc/c-client.cf'}3 |
| | | | EVENIL MDIEE | {'file': '/usr/local/libexec/imapd'}3 |
| | | {'subject': 'wget'}3 | EVENT_WRITE | |
| | | | EVENT_WRITE | {'netflow': '128.55.12.166:47081'}3 |
| | | | EVENT_RECVFROM | {'netflow': '193.40.5.73:80'}3 |
| | | | | |