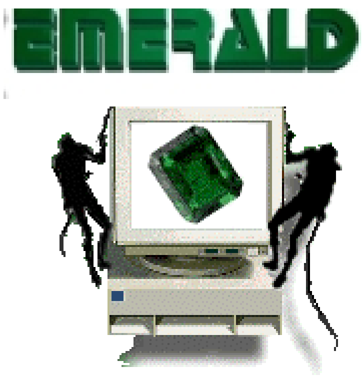

EMERALD™ *eXpert-BSM*™ Evaluation Edition

http://www.sdl.sri.com/emerald/

Sun Solaris Host-Based Intrusion Detection System

System Design Laboratory

SRI International

Release Date: April, 2002

User's Guide, Version 1.5

EMERALD(TM)
(Event Monitoring Enabling Responses to Anomalous Live Disturbances)

Table of Contents

1 Notice to Users

eXpert-BSM is a host-based intrusion detection solution for Sun Solaris operating platforms, representing one component in a suite of advanced intrusion detection technologies developed by the EMERALD Development Team at SRI International. See our Web site http://www.sdl.sri.com/emerald/ for additional information.

Before You Start

You should not attempt to install or operate the EMERALD *eXpert-BSM* host intrusion detection monitor without first reading this document. This document describes the proper system preparation, installation, policy configuration, important caveats, and results expectations, which are critical to successfully operating this component. To lessen your burden, we've tried to be as concise as possible in the material that follows, so please invest some time to read this manual. We have included a **Quickstart** section for your convenience, but that should not be viewed as a substitute for reading the rest of this document.

About the Evaluation Edition

SRI provides this release of *eXpert-BSM* as a stand-alone intrusion detection system for Sun Microsystems Solaris operating systems for use on a single host system for internal evaluation purposes only. For more information regarding advanced features and technical support, please contact **emerald@sdl.sri.com**. For those who would like to license this component for operational deployment in multi-host, enterprise-wide deployments, we provide a full-featured, advanced version of eXpert-BSM, which includes the following features:

- Multi-host alert management – with additional components, users can consolidate and analyze alerts from a suite of distributed *eXpert-BSM* or other EMERALD monitors.

- DBMS services – users can manage and view alerts from a distributed suite of *eXpert-BSM* or other EMERALD monitors using our relational database interface component. We currently support Oracle and Postgres.

- Alert translation services – additional EMERALD components allow users to translate EMERALD alert reports into a variety of binary and ascii formats.

- eResponder™ – a countermeasure invocation system, tightly coupled with *eXpert-BSM*, which provides both automated and manual response directive execution. [under development]

Value-added services from SRI – the EMERALD development team can also be engaged for these additional services associated with use of eXpert-BSM:

- Consulting services – SRI can negotiate contracts for technical support, consulting services, and feature extensions for use with this and other EMERALD components.

- Knowledge-base updates – licensed users will receive any updates to the eXpert-BSM intrusion detection knowledge-base produced by SRI.

To find outmore about the advanced version of eXpert-BSM for production use in multi-host deployments, please contact emerald@sdl.sri.com.

2 Quickstart

This section is intended as a checklist for the minimum steps required to start *eXpert-BSM*, and is provided for your convenience. To utilize the full potential of *eXpert-BSM*, you must read the remainder of this document.

1. Check the System Requirements, especially with respect to Solaris bugs and patches.

2. Before installing eXpert-BSM, you must enable BSM auditing. See Enabling Solaris Audit Module for more information on BSM audit configuration.

3. Untar the package amd in the `_BSM` directory using the user account from which you will run eXpert-BSM (not root). You need to know the name of a group that is allowed to run the monitor, and the path to your Java installation.

4. Move to the `$install/_BSM/` directory, su to root, and as root run the install script `Install_eXpert_BSM`.

5. Go into the `resource-object/config` directory. In the file `local_netmap.conf` you need to specify what hosts are internal, see Configuring the Local Network Address List. In file `eXpert-Config.inc`, at least list the administrators in the parameter BSM_ADMINISTRATIVE_USER_LIST, see Configuring the eXpert-BSM Knowledge-Base.

6. As a user in the group specified during installation, go into the `_BSM` directory, and run `Run_eXpert_BSM`. The three operating modes are described in Operating Instructions.

7. The results will show up in the `_BSM/results` directory, and in the GUI if you chose to enable and start it.

8. To confirm that the monitor is working in real-time mode, try the following: In a separate session, login (not su) as a user not listed as an administrator. Let that user su to a user who is listed as an administrator. That should result in an alert from the monitor. See Appendix I for additional ways to generate alerts.

9. To shut down the GUI, go to the File menu and choose Exit. To shut down the monitor, run `_BSM/Shutdown_eXpert_BSM`.

3 EMERALD eX*pert-BSM* Overview

What is eXpert-BSM?

eXpert-BSM, EMERALD's host-based intrusion detection monitor for Solaris BSM audit trails encapsulates the most comprehensive knowledge-base for detecting misuse in host audit trails that has ever been fielded. Section 4, *eXpert-BSM* Detection Summary, enumerates the warning and attack heuristics available to the *eXpert-BSM* inference engine. *eXpert-BSM* is packaged and distributed as a stand-alone intrusion detection service for detecting insider misuse and security policy violations on Sun Solaris operating systems.

The EMERALD *eXpert* (pronounced E-expert) is a highly targetable signature-analysis engine based on the expert system shell P-BEST. Under EMERALD's eXpert architecture, event-stream-specific rule sets are encapsulated within resource objects that are then instantiated with an EMERALD monitor, and which can then be distributed to an appropriate observation point in the computing environment. This enables a spectrum of configurations from lightweight distributed eXpert signature engines to heavy-duty centralized host-layer eXpert engines, such as those constructed for use in eXpert's predecessors, NIDES (Next-Generation Intrusion Detection Expert System), and MIDAS (Multics Intrusion Detection Alerting System). In a given environment, P-BEST-based eXperts may be independently distributed to analyze the activity of multiple network services (e.g., FTP, SMTP, HTTP) or network elements (e.g., a router or firewall). As each EMERALD eXpert is deployed to its target, it is instantiated with an appropriate resource object (e.g., an FTP resource object for FTP monitoring), while the eXpert code base remains independent of the analysis target. For more information about the eXpert inference engine design, capabilities, and language, see

http://www.sdl.sri.com/emerald/pbest-sp99-cr.pdf.

What is EMERALD?

The *EMERALD* (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment is a distributed scalable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. It combines models from research in distributed high-volume event correlation methodologies with over a decade of intrusion detection research and engineering experience. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various layers within a network computing environment (OS, application, network service, TCP/IP). These monitors contribute to a streamlined event-analysis system that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet. The EMERALD project represents a comprehensive attempt to develop an architecture that inherits well-developed analytical techniques for detecting intrusions, and casts them in a framework that is highly reusable, interoperable, and scalable in large network infrastructures.

A key aspect of this approach is the introduction of the EMERALD monitors. An EMERALD monitor is dynamically deployed within an administrative domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and service (privileged subsystems with network interfaces). An EMERALD monitor may interact with its environment passively (reading activity logs) or actively via probing to supplement normal event gathering. As monitors produce analytical results, they disseminate these results asynchronously to other client EMERALD monitors. Client monitors may operate at the domain layer, correlating results from service-layer monitors, or at the enterprise layer, correlating results produced across domains. Under the EMERALD framework, a layered analysis hierarchy may be formed to support the recognition of more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an enterprise.

The monitors themselves stand alone as independently tunable, self-contained analysis modules with a well-defined interface for sharing and receiving event data and analytical results with third-party security services. An EMERALD monitor performs either signature analysis, or probabilistic anomaly detection or both, on a target event stream. EMERALD's signature analysis subsystem employs a variant of the P-BEST expert system, which allows administrators to instantiate a rule set customized to detect predefined "problem activity" occurring on the analysis target.

Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. The event stream is derived from a variety of sources, including audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion detection instrumentation. The event stream is parsed, filtered, and formatted by the target-specific event collection methods provided by the monitor's pluggable configuration library referred to as the *resource object*. Event records are then forwarded to the monitor's analysis engine(s) for processing. For more information regarding the EMERALD design, see http://www.sdl.sri.com/emerald/emerald-niss97.html.

4 *eXpert-BSM* Detection Summary

The eX*pert-BSM* knowledge-base represents the most sophisticated and comprehensive collection of audit-based intrusion detection heuristics ever assembled under a single host-based intrusion detection system. The majority of these heuristics focus on detecting the underlying compromises that occur within and across attack methods relevant across Unix hosts. Where possible, rules are implemented to provide the most general coverage for misuse detection and security policy violations to cover the widest range of attack classes possible from audit-based analysis. These rules have been extensively tested for their ability to recognize the intrusive activity described below, as well as avoiding false positives. See Configuring eXpert-BSM for more information on how to configure the rule parameters for this knowledge-base.

The following is a snapshot of the EMERALD *eXpert-BSM* knowledge-base for warnings and intrusion indicators as of the date of this release.

The EMERALD team continues to actively extend our current knowledge sets for both host- and network-based monitors. Our EMERALD software distribution web page **http://www.sdl.sri.com/emerald/releases**, has further information regarding subsequent releases.

The following attack heuristics are available within the release of this component:

- **BSM_Root_Core_Creat**: BSM Monitor observed the creation of a root core file. There are multiple known attacks that exploit or generate, as a side effect, root-owned core files, and some attacks that are formulated to ensure that the core file will include content from the shadow password file.

- **BSM_Reach_Max_BadLogin**: BSM Monitor observed N (default = 4) failed login attempts. If the username was invalid, the "user" field contains "invalid username." Otherwise, this represents a series of bad login attempts. (config: `BSM_MAX_LOGIN_THRESHOLD, BSM_FAILED_LOGIN_WINDOW`)

- **BSM_Root_Core_Event**: BSM Monitor observed a root process suffering a core dump. This event occurs commonly as a result of root process subversion or attacks designed to shut down root services. The kernel itself detects the event. It does not indicate core file creation, or the location of that core file, which may or may not occur.

- **BSM_FTP_Passwd_Guesser**: BSM Monitor observed N (default = 4) failed login attempts via the FTP daemon. If the username was invalid, the "user" field contains "invalid username." Otherwise, this represents a series of bad passwords submitted for a user's account. (config: `BSM_FAILED_LOGIN_WINDOW, BSM_MAX_FTP_BADPASSWORDS`).

- **BSM_FTP_Username_Guesser**: BSM Monitor observed a series of attempts to submit invalid usernames to the FTP daemon. The FTP daemon responds differently when an invalid account name is submitted. This allows someone to repeatedly attempt FTP logins until a valid name is discovered. (config: `BSM_MAX_FTP_BADPASSWORDS, BSM_FAILED_LOGIN_WINDOW`).

- **BSM_Suspicious_Exec_Argument**: BSM Monitor is capable of recognizing file accesses with arguments that match a set of known attack names. This is just an indicator that the record is worthy of inspection, and is not an attack trigger. (config: `BSM_SUSPICIOUS_EXEC_LIST`).

- **BSM_Time_Warp**: BSM Monitor observed a movement in local host time greater than N seconds (default = 10 min). This is a potential indicator of someone attempting to hide his or her tracks after penetrating a system. (config: `BSM_MAX_BACKWARD_TIME`).

- **BSM_Root_Core_Access**: BSM Monitor observed an access to a root core file by a non-administrative user. There are known exploits that allow access to the shadow password files by causing a root core dump directly after a failed USER login request.

- **BSM_Access_Private_File**: BSM Monitor raises a warning indicator when a "private" file (in a non-public location) is altered by someone other than the file owner. (config: `BSM_USER_HOMES_LOCATIONS`).

- **BSM_Mod_System_Resource**: BSM Monitor raises an alert indicator when a *nonreserved* account user alters a system resource log file. This is a highly general heuristic for recognizing common actions that occur after compromise. (config: `BSM_SYSTEM_RESOURCE_FILES, BSM_LAST_RESERVED_ACCOUNT, BSM_SYSTEM_LOG_LOCATIONS`).

- **BSM_FTP_Anon_Write**: BSM Monitor observed an anonymous user modifying the filesystem (e.g., writing, deleting, directory creation, chmod). When a file is written, the filename is registered in the fact-base and employed by BSM_FTP_Warez_Activity. (config: `BSM_ANON_FTP_MONITOR_WINDOW, BSM_LOCAL_FTP_UID`).

- **BSM_FTP_Warez_Activity**: BSM monitor observed N anonymous users retrieving an anonymously uploaded file that has been registered by the BSM_FTP_Anon_Write rule. (config: `BSM_ANON_FTP_MONITOR_WINDOW, BSM_FTP_WAREZ_COMPLAINT, BSM_LOCAL_FTP_UID`).

- **BSM_Client_INET_Watch**: BSM Monitor observed a flood of inetd-based connections from a remote location. These include in.telnetd, in.ftpd, and in.fingerd. The process table attack is an example exploit for this rule set. (config: `BSM_SUSPICIOUS_EXEC_LIST`).

- **BSM_Proc_Exhaust_Threshold**: BSM Monitor observed process resource exhaustion. This heuristic provides threshold analysis on failed forks. (config: BSM_MAX_FAILED_PROCS_PER_CYCLE, BSM_FAILED_PROC_THRESHOLD_WINDOW)

- **BSM_File_Exhaust_Threshold**: BSM Monitor observed a series of failed write operations that were rejected for lack of available filesystem space. (config: BSM_MAX_NOSPACE_ERRORS, BSM_WRITE_ERR_THRESHOLD_WINDOW)

- **BSM_Attempted_Root_Login**: BSM Monitor observed a failed attempted **`root`** login via login, telnet, rlogin, rsh, su. With BSM installed, direct root login is disallowed. Administrators are required to login under their own accounts, and transition to **`root`** via su(1).

- **BSM_Suspicious_Setuid**: BSM Monitor observed that the setuid bit has been enabled by a non-administrative user (i.e., a process whose original login ID is not a known administrator). If the user enabling the setuid bit owns the file, then a warning is raised. If the user enabling the setuid bit is not the owner of the file, then this alert is flagged as an attack (clear authority violation). This is an excellent heuristic for recognizing common actions that occur during an intrusion, where the attacker subverts the system into enabling the setuid bit on a root-owned file. This heuristic also distinguishes between administrative users and non-adminstrative users. (config: `BSM_ADMINISTRATIVE_USER_LIST`).

- **BSM_Setreuid_By_Nonadmin**: The BSM Monitor observed a non-administrative user process changing its real user ID to an administrator ID. (config: `BSM_ADMINISTRATIVE_USER_LIST`).

- **BSM_Suspicious_Port_Probing** [1]: Applicable to Solaris 2.6 and above. The BSM Monitor observed a remote host attempting to connect to a series of service ports that collectively indicate a potential selective port scan. (config: `BSM_PORT_ANALYSIS_WINDOW`).

- **BSM_Bad_Port_Connection** [1]**:** BSM Monitor allows specification of a set of network ports that should not be accessed be external clients. BSM Monitor raises an alert when external connections to these ports occur, including the requestor IP address. (config: `BSM_UNACCEPTABLE_PORT_CONNECTIONS`).

- **BSM_Buffer_Overflow_Exec**: BSM Monitor observed a buffer overflow attack. This could triggered by eject, fdformat, ffbconfig, rdist, or several other known buffer overflow attacks. It covers the entire class of SUID stack smashing on local applications at initialization.

- **BSM_Special_User_Exec**: Some reserved accounts are not intended to run processes, but rather are present for file ownership purposes. The BSM Monitor raises an alert if it identifies an `exec()` call from a reserved account. (config: `BSM_EXEC_LESS_ACCOUNTS).`

- **BSM_Exec_Non_Author**: BSM Monitor raises an alert if it identifies an exec() call from a setuid process, such that the exec'd file is a program not owned by root or the SUID user. (config: BSM_LAST_RESERVED_ACCOUNTS)

- **BSM_Change_User_Environ_File**: BSM Monitor observed the contents of a user's environment files being modified by another user. This is a highly general heuristic for recognizing common actions that occur after compromise. (config: BSM_USER_ENV_FILES)

- **BSM_Illegal_Shadow_Passwd_Access**: BSM Monitor observed destructive access to the OS password/shadow file occurring through an unknown facility and non-administrative user. (config: BSM_ADMINISTRATIVE_USER_LIST)

- **BSM_Mod_System_Executable**: BSM Monitor observed the alteration of a system executable. It catches attempts to modify system binaries. This is a highly general heuristic for recognizing common actions that occur after compromise. (config: BSM_SYSTEM_BIN_LOCATIONS).

- **BSM_Root_By_NonAdmin**: BSM Monitor is capable of maintaining a list of who is and is not allowed to acquire administrative privilege. When a non-administrative user acquires privilege (via any facility), this alert is raised. In systems with no strong policy about who is allowed to acquire root, this facility can be disabled. (config: BSM_ADMINISTRATIVE_USER_LIST)

- **BSM_Read_Private_File:** BSM Monitor allows users to specify sensitive file lists and associate with those lists groups of users who are and are not allowed to reference files in the lists. For more information, see Setting a Monitoring Policy, Configuring *eXpert-BSM*.

- **BSM_Write_Private_File**: BSM Monitor allows users to specify sensitive file lists and associate with those lists groups of users who are and are not allowed to modify or destroy files in the list. For more information, see Setting a Monitoring Policy, Configuring *eXpert-BSM*.

- **BSM_Dissallowed_FTP_Read:** BSM Monitor observed an FTP process reference the content of a file in violation of the site survieillance policy. For more information, see Setting a Monitoring Policy, Configuring *eXpert-BSM*.

- **BSM_Dissallowed_FTP_Write:** BSM Monitor observed an FTP process modify the content of a file in violation of the site survieillance policy. For more information, see Setting a Monitoring Policy, Configuring *eXpert-BSM*.

- **BSM_Illegal_Execution**: BSM Monitor allows users to specify lists of binaries and shell scripts and associate with those lists groups of users who are and are not allowed to execute the programs in the list. For more information, see Setting a Monitoring Policy, Configuring *eXpert-BSM*.

- **BSM_Promiscuous_Mode**: BSM Monitor observed a process open a promiscuous mode port (e.g., a sniffer), and reports the promiscuous mode event if the user is not an admin: (config: `BSM_ADMINISTRATIVE_USER_LIST, BSM_EMERALD_NIC_NAMES`)

- **BSM_Self_Echo_Alert**: BSM Monitor observed a self-ping DoS attack. (config: `BSM_MAX_ECHOS_RECEIVED, BSM_ECHO_FLOOD_WINDOW`)

- **BSM_Inetd_Subversion**: BSM Monitor observed that an inetd service executable has been overlayed in an illegal manner. This indicates that a root-privileged service has been subverted, for example via a data segment buffer overflow. Examples include the Solaris sadmin data segment overflow exploit. (config: `BSM_TCP_WRAPPER`).

5 System Requirements

Operating System

The EMERALD *eXpert-BSM* Monitor requires a Sun Microsystems Sparc platform running one of:

- SunOS 5.6 (Solaris 2.6), service patch 105621-24 or newer
- Solaris 7, service patch 106541-12 or newer
- Solaris 8, service patch 108875-07 or newer

The EMERALD *eXpert-BSM* monitor generally consumes around 5-12MBs of process space. We recommend running *eXpert-BSM* on machines with 64MBs or more of memory and 20MBs or more of available disk space on a local drive. For more information on expected process growth, refer to the *eXpert-BSM* FAQ:

http://www.sdl.sri.com/emerald/releases/expert-BSM/faq.html

Caution: Solaris Bugs

If you are attempting to install *eXpert-BSM* on certain versions of Solaris, you must ensure that the appropriate patches are installed before you try to run *eXpert-BSM*. The OS bugs listed below could render your system **unusable** when triggered by *eXpert-BSM*. Use `'showrev -p'` to see what patches are installed, and if needed, visit the Sun Microsystems web page http://sunsolve.sun.com for information on bugs and patches.

Sun Bug ID	Description	Possible Patch (OS)
4194454	auditing to pipe causes system to panic	105621-24 (5.6) 106541-12 (5.7)
4229414	Solaris 7 64 bit BSM auditing with +argv policy break exec()	106541-12 (5.7)
4307306	stopping c2 auditing does not always stop auditing in the kernel	105621-24 (5.6) 106541-12 (5.7) 108875-07 (5.8)

In addition, there are problems in Solaris 8 (SunOS 5.8) that require patches to be applied for eXpert-BSM to function properly. Those are also covered by patch 108875-07 or newer.

Java environment

The EMERALD Alert Management Interface requires the use of the JAVA Development Kit (JDK) 1.1.8, which in most cases is installed as part of your standard Sun Solaris installation package. If Java JDK 1.1.8 is not installed on your Solaris platform, you can obtain this package directly from Sun Microsystems at http://www.sun.com/solaris/java.

6 Download Instructions

Evaluation versions of EMERALD eX*pert-BSM* are available for download to those who apply for registration on our download request page on the following URL:

http://www.sdl.sri.com/emerald/releases

By registering your contact information on this page and agreeing to the Software Distribution Agreement and Reporting and Feedback Agreement, you will receive within 5 business days an email message with an appropriate password to decrypt the *eXpert-BSM* binary release. The binary will require decryption using the GNU Privacy Guard algorithm (available from our registration page or from www.gnupg.org). The release will also require Solaris uncompress and tar.

7 Contents of Distribution

The following files are contained in this distribution of the EMERALD *eXpert-BSM* Monitor (indentation indicates containment).

doc	*Documentation directory*
Emerald-AMI…pdf	Java GUI User's Guide
user-manual_1_2.pdf	*This user document*
copyright	*EMERALD copyright information*
license.pdf	*License and distribution information*
PBEST-1999-…pdf	*Technical article about P-BEST*
_BSM	*EMERALD control directory*
Install_eXpert_BSM	*Installation script (run as* ***root****)*
Run_eXpert_BSM	*Startup script*
Run_config	*Start Configuration GUI*
Shutdown_eXpert_BSM	*Shutdown script*
Start_GUI	*Alert GUI start script*
_bsm_to_ebin	*Convert BSM file to EMERALD binary file*
_ebin_to_ascii	*Convert EMERALD binary file to ASCII*
eXpert-config.sh	*Run_eXpert_BSM parameter config file*
autoboot/auto_start	*autoboot start script*
autoboot/auto_stop	*autoboot stop script*
bin	*Solaris 2.6 thru 2.8 executables*
SunOS-5.*	*EMERALD executables directory*
ask_yn	*Utility script*
ebsmgen	*BSM-to-EMERALD data converter*
ebsmprobe	*Real-time BSM data retrieval*
ebsmsetpolicy	*Utility to set the BSM audit policy*
emsgdump	*Results file dump utility*
eXpert-BSM	*EMERALD expert-system BSM analyzer*
slay	*Utility script for killing processes*
throttle	*I/O buffering process*
resource-object/config	*Monitor configuration directory*
accesspolicy.conf	*Surveillance policy configuration*
eXpert-Config.inc	*Knowledge-base configuration*
local_netmap.conf	*local IP address map*
username_map.conf	*User-ID to user-name map (built at install time)*
_BSM/results	*Results and log directory*
bsm-alerts-*.resolver	*EMERALD binary format alerts file*
bsm-expert-*.log	*ASCII console alerts and error log*
bsm-generator-*.log	*BSM data converter log*
gui	*This directory contains the EMERALD GUI subsystem for JAVA 1.1.8*
*	
samples	*An extensive battery of BSM records (encoded in EMERALD binary format) that exercise the eXpert-BSM knowledge-base*
emerald-attack-battery.ebin	

8 Pre-Installation Cautions and Caveats

What You Need Before Installation

- Root privilege is required to install eX*pert-BSM* for real-time operation. If you wish to limit the use of this component to batch-mode operation, root privilege is not required.

- We strongly recommend that you install eX*pert-BSM* on the target host's local hard drive rather than an NFS mounted partition when operating this system in real-time mode. This is due to both performance and reliability concerns.

- Certain versions of the Solaris operating systems require certain service patches from Sun Microsystems (see the section on Solaris Bugs).

- The EMERALD Alert Management Interface (GUI) requires the use of the JAVA Development Kit (JDK) 1.1.8, which must be installed on your system and accessible to the account from which you will run EMERALD.

9 Installing *eXpert-BSM*

Enabling Solaris Audit Module

Solaris auditing must be configured for auditing before *eXpert-BSM* is installed. This can be done as follows:

1. Make sure that users are logged off. Log in on the console as root. Reboot the system and from the console, log into the system in single-user mode by using `telinit` (see init(1M) man page).

```
# /etc/telinit 1
```

2. In single-user mode, change directory to `/etc/security` and run `bsmconv.`

```
# cd /etc/security
# ./bsmconv
```

This process creates an audit_startup file. Upon completion of bsmconv, you will be prompted to reboot—DO NOT reboot until instructed to do so in step 5.

3. Rename `/etc/security/audit_startup` to something else, see example below. This is to prevent the audit daemon from starting at system boot. The *eXpert-BSM* installation contains ebsmprobe, which is a replacement for auditd.

```
# mv /etc/security/audit_startup   \
 /etc/security/audit_startup.we_dont_want_auditd_to_start
```

4. If there is a line

```
set abort_enable = 0
```

in `/etc/system`, you might want to comment it out by making the first character of the line a star (*). This line is added by bsmconv in Solaris 2.6 and later to disable STOP-A halting. It adds marginal security to a desktop machine, but is inconvenient when you need to halt a server from the console.

5. Reboot the system into multiuser mode.

```
# /usr/sbin/reboot
```

6. Running the following command as root after reboot should indicate `"audit condition = unset".`

```
# /usr/sbin/auditconfig -getcond
```

For more information, consult the "SunShield Basic Security Module Guide" for Solaris, available from http://docs.sun.com.

Security Recommendation

eXpert-BSM requires privilege only to capture the audit records from the kernel. This privileged function has been isolated into an independent probe process, which can be granted setuid capability independently from the rest of the *eXpert-BSM* process chain. We recommend the following setup strategy (advisory only, not required):

1. Create an exclusive account for running *eXpert-BSM*, called `emerald`, and an exclusive group with the same name.

2. Extract the *eXpert-BSM* package into the target `$Install` directory owned by the `emerald` account.

3. Limit accessibility of the directory to the `emerald` account.

Setup Instructions

Log in with root privilege, invoke the script `$Install/_BSM/Install_eXpert_BSM` and follow the directions.

Note: The eXpert-BSM process chain does not audit itself. There is no need to configure `/etc/security/audit_user` to exclude user `emerald`.

Installation Sample Dialog with Explanation

This section describes the individual steps involved in the installation of *eXpert-BSM*. Additional commentary is numbered. To begin installation, login as root and move to directory `$Install/_BSM/`. From there, run

```
# ./Install_eXpert_BSM
```

1. This script first attempts to determine if the installation host is running Solaris 2.6 or newer. If it is not, the following message appears:

```
 ===========================================================
Unsupported operating system: X
This version of the EMERALD BSM Monitor is designed for"
Solaris 6, 7, and 8
```

2. If this operating system is supported by this release, the following banner is shown:

```
*****************************************************
==========================================================

eXpert-BSM BSM monitor installation: <timestamp>


 *********************************************************
 *                                                       *
 *                      EMERALD (tm)                     *
 *   (Event Monitoring Enabling Reponses to Anomalous    *
 *                   Live Disturbances)                  *
 *                                                       *
 *         copyright 1996-2002 SRI International         *
 *                                                       *
 *   This is an UNPUBLISHED work of SRI International    *
 *   and is not to be used, copied or disclosed except   *
 *   as provided in the Software Distribution Agreement  *
 *   with SRI International.                             *
 *                                                       *
 *      EMERALD, eXpert-BSM, eXpert-Net, eXpert-HTTP,    *
 *    eXpert-SMTP, eXpert-TCP, eXpert-UDP, eXpert-FTP,   *
 *       eXpert-ARP, eXpert-Session, eXpert-ICMP,        *
 *         eBayes-TCP, M-Correlator, eAggregator         *
 *          are Trademarks of SRI International          *
 *********************************************************
```

Hit return to continue...

```
Attention: You are about to install the EMERALD (TM) BSM Monitor
intrusion detection monitor into your system.  This component
is designed for Solaris 6 thru 8 operating systems (32/64 bit)
with audit facilities installed.  If you have not installed the
Solaris audit facilities on this machine, please abort this
installation and install audit facilities first.

You may ctrl-C out of this script at any time if you do not
wish to continue the installation.


It is extremely important that you have read Sections 8, 9

and 10 of the eXpert-BSM User Manual before attempting to install
and operate this system.  If you have not read these sections,
please read them before continuing.
```

```
Have you reviewed these section (Y/N)?
```

To stop execution of the script, hold down the control key while hitting c, and then press return.

You will be asked a question whether you have reviewed this documentation. If you answer no, the script will exit and will indicate that you should review Sections 8, 9, and 10 of this document.

3. `Install_eXpert_BSM` will provide a warning message to inform you about patch requirements for Solaris:

```
============================================================
WARNING: This operating system is SunOS-5.7 in 64-bit mode.
It could have the following serious bugs:

Sun Bug ID | Description                       | Possible Patch
----------------------------------------------------------------
 4194454   | auditing to pipe causes system    | 105621-24 (5.6)
           | to panic                          | 106541-12 (5.7)
----------------------------------------------------------------
 4229414   | Solaris 7 64 bit BSM auditing     | 106541-12 (5.7)
           | with +argv policy break exec()    |
----------------------------------------------------------------
 4307306   | stopping c2 auditing does not     | 105621-24 (5.6)
           | always stop auditing in the       | 106541-12 (5.7)
           | kernel                            | 108875-07 (5.8)
----------------------------------------------------------------
```

It is VERY IMPORTANT that you make sure that the appropriate patches are installed before you try to run eXpert-BSM. The OS bugs listed above could render your system UNUSABLE when triggered by eXpert-BSM. Use 'showrev -p' to see what patches are installed. See also http://sunsolve.Sun.COM/ for information on bugs and patches.

Do you wish to continue the installation (Y/N)?

You can use the Solaris showrev command to verify that you have a properly patched installation of Solaris before proceeding. If you answer no, the script will exit.

4. `Install_eXpert_BSM` verifies that you are operating as user root. Root is required to modify the audit configuration and enable real-time access to kernel audit data. If you are not root, you will see the following message:

```
============================================================
WARNING: Installation process should be run as root.
```

```
Do you wish to continue (y/n)?
```

If you wish to employ eXpert-BSM for real-time use, type 'n' to exit this installation script, become root, and restart the installation process. If you intend to use eXpert-BSM exclusively for batch mode processing, you may type ‘y’ and continue.

Please note that when you do not run as root, the script cannot correctly determine whether BSM is enabled on your system, and you will again be asked whether you want to continue.

5. The installation script automatically constructs the file `username_map.conf`, which is located in `$Install/resource_object/config/.`

```
============================================================
Now building the first-cut user-name map file.
```

As you add new accounts to your environment, you may wish to re-run this install program to add the additional usernames and IDs.

```
Note: if you are not running yp, you may encounter a
      yppasswd-related error.  Just ignore this error.
```

Would you like to edit the username map (usually not necessary) (Y/N)?

The `username_map.conf` is automatically generated by the installation script and provides eXpert-BSM with a mapping between Subject IDs and human-readable usernames. Both the local `/etc/passwd` file and the NIS (yp) passwd database are used as input. This resulting map allows eXpert-BSM to avoid performing expensive name lookups at runtime, as it receives audit records. Here is an example of the username map file:

```
      root      0
      daemon    1
      bin       2
      sys       3
      adm       4
      lp        71
      uucp      5
      nuucp     9
      listen    37
      operator  28
      johnny    443
      suzie     445
```

Updating the username map: After you have added or deleted user accounts on the system, there are two ways to update the username map. Once you have completed modifications, you may activate these configuration changes by sending a SIGHUP to the eXpert-BSM process:

Edit the file with a text editor, or simply rerun the install script. The username_map will be rebuilt.

If you answer yes the script will prompt you for the editor you wish to use.

```
============================================================
Enter the editor you wish to use (default: vi)

If you press enter, your default editor will be used.

============================================================
Now entering the editor vi on the user-name map file.
Make any adjustments to the file, save it, and exit the
editor to continue with the installation...

When you are done, the script will reply as follows:

Welcome Back: If you need to modify the usermap file again, it
     can be found in ./resource-object/config/username_map.conf.
     For more information on username_map.conf, see the
     user documentation.
```

6. eXpert-BSM requires privilege to capture the audit records from the kernel. This privileged function has been isolated into an independent probe process called ebsmprobe.

```
============================================================
The eXpert-BSM startup requires root privilege for:
ebsmprobe realtime BSM data retrieval code

Do you wish to allow set-UID-to-root for ebsmprobe (Y/N)?
```

7. You are prompted to enter the group name of the individual(s) needing access to the eXpert-BSM results. For example, if eXpert-BSM will be operated under the emerald group, then type `emerald.`

```
Use of eXpert-BSM should be restricted to a limited group of us-
ers. Enter the group name or username that will be allowed
to run the BSM monitor (e.g., emerald):
```

8. The script checks whether the audit daemon is currently running. If it is, you are prompted to shut it down. If you do not wish to run eXpert-BSM in real-time mode, you could restart auditd after the install script is finished

```
============================================================
ps indicates that auditd is running:
auditd must be shutdown to initialize EMERALD.
```

```
Do you wish to shutdown the audit daemon (Y/N)?
```

If you agree to terminate the process, the following command is run.

```
# /usr/sbin/audit -t
```

9. eXpert-BSM determines whether the audit daemon is currently set to start at boot time on your system. This should not be the case if you want to run in real-time; as eXpert-BSM real-time mode does not work in parallel with the Solaris audit daemon. Type 'Y' to continue with the installation process. To later re-enable the Solaris audit daemon to start at boot time, simply rename the file `audit_startup.renamed_by_emerald` file back to `audit_startup`.

```
============================================================

eXpert-BSM has determined that auditing is currently enabled
on your system and that auditd will continue to be enabled
on system reboot.  Note: In real-time mode eXpert-BSM cannot

operate in parallel with auditd, so disabling auditd facilitates
the regular use of eXpert-BSM.

Details:
    to disable auditd from automatically restarting at system
    reboot, this script will rename the audit_startup script
    from
          /etc/security/audit_startup
    to
          /etc/security/audit_startup.renamed_by_emerald.


Do you wish to rename the audit script (y/n)?
```

10a. eXpert-BSM attempts to install a custom audit configuration.

```
============================================================
eXpert-BSM provides a highly optimized BSM configuration, which
reduces CPU load and is required to function properly.  You can
optionally back up your current configuration before the eXpert-
BSM configuration is installed.
```

10b. eXpert-BSM needs to modify the audit configuration of your Solaris host. Selecting **Y** (yes) stores your previous files in a file called `/etc/security/orig_audit_file`{timestamp}`.tar`.

```
Do you wish to back up your current BSM configuration (Y/N)?
```

10c. eXpert-BSM will prompt you to remove the default audit configuration files. Assuming you select ‘Y’ to question 10b, you will be able to later restore the original Solaris configuration files should you choose to uninstall eXpert-BSM, see Uninstalling eXpert-BSM.

```
BSM configuration files
  /etc/security/audit_class /etc/security/audit_control
  /etc/security/audit_event /etc/security/audit_user
  have been BACKED UP to
  /etc/security/orig_audit_01Jun21-0731.tar.Z
```

Next, the install script will ask to remove the old BSM configuration files.

```
============================================================
The BSM configuration files
/etc/security/audit_class /etc/security/audit_control
/etc/security/audit_event
/etc/security/audit_startup.renamed_by_emerald
/etc/security/audit_user /etc/security/audit_warn
/etc/security/audit_data
will be deleted.

OK to delete (Y/N)?
```

11. eXpert-BSM unloads and installs the following files into `/etc/security`/:

```
     audit_class
     audit_control
     audit_event
     audit_user
```

The files are located in `$Install/resource-object/audit_config.tar` for your inspection.

```
Install EMERALD BSM configuration files (Y/N)?
```

12. The files discussed in (11) are moved to `/etc/security`/, and permissions are set appropriately.

13. You may enable eXpert-BSM to automatically startup during the system boot process:

```
============================================================
eXpert-BSM Autoboot Installation:

You have the opportunity to configure eXpert-BSM to automatically
start during the boot procedure.  If you elect to enable
eXpert-BSM to automatically start at system boot, the following
files will be created: 1) sh script /etc/init.d/eXpert-BSM,
2) symlink /etc/rc2.d/S80eXpert-BSM which points to the sh script,
and 3) alert log directory /var/adm/securityd/.

To temporarily disable eXpert-BSM autoboot mode, we recommend you
rename /etc/rc2.d/S80eXpert-BSM to /etc/rc2.d/disabled-S80eXpert-
BSM.
See Section 9 for more details.


Do you wish to enable eXpert-BSM autoboot mode (Y/N)?
```

14. This completes the installation phase. Before running eXpert-BSM you must follow the configuration phase discussed in Configuring *eXpert-BSM*.

```
============================================================


eXpert-BSM installation phase complete.
Configuration Phase is required before running eXpert-BSM

Please refer to Section 10 of the eXpert-BSM User Manual for
information on configuring this component.  The following
configuration files should be configured before running eXpert-
BSM:

     {emerald_install}/_BSM/eXpert-config.sh
     {emerald_install}/resource-object/config/accesspolicy.conf
     {emerald_install}/resource-object/config/eXpert-Config.inc
     {emerald_install}/resource-object/config/local_netmap.conf
     {emerald_install}/resource-object/config/username_map.conf


 ************************************************************


Do you wish to configure eXpert-BSM now? (Y/N)?
```

Now that you have completed installation, proceed to Chapter 10 for information on properly configuring eXpert-BSM for you environment.

10 Configuring *eXpert-BSM*

eXpert-BSM provides an unprecedented degree of dynamically adjustable user control over its runtime operation. However, this greater user flexibility also implies greater responsibility on you, the user, to fully understand how to configure this engine for your needs and environment.

After completion of the installation phase of eXpert-BSM, described in the previous section, you must perform the eXpert-BSM configuration phase. While we provide generally applicable default values, some aspects of the configuration process requires customization to your environment before eXpert-BSM can properly operate. The configuration phase of eXpert-BSM proceeds as follows:

- Configuring the Run_*eXpert-BSM* Script: sets various external parameters to control the settings for your local time, debug mode, script prompt invocations, IDIP alert production, and socket use.

- Configuring the *eXpert-BSM* Knowledge-Base: provides the user unprecedented control over the intrusion detection heuristics. Required for proper operation of eX*pert-BSM*.

- Configuring the Local Network Address List: provides eX*pert-BSM* a list of internal IP addresses for use in network-related heuristics.

- Configuring the Surveillance Policy for Local File Access: (optional) provides an optional configuration facility for specifying an access policy to be monitored by eX*pert-BSM*.

Configuring the Run_eXpert_BSM Script

eXpert-BSM is run through the csh script `$Install/_BSM/Run_eXpert_BSM` script. See Operating Instructions for more information on using `Run_eXpert_BSM`. The following settings are available for modification through file `$Install/_BSM/eXpert-config.sh`, which is referenced by `Run_eXpert_BSM`.

- This variable will cause the Run_eXpert_BSM script to run silently, with no user command prompts. This overrides all interactive settings below except CHECK_EFUNNEL. If set to "off", then by default the GUI will not be invoked and the results directory will *not* be cleared.Values: "on", "off", "yes", "no”

    ▪ **`set Interactive = "on"`**

- SETTING LOCAL TIME ZONE: You can set the default timezone as appropriate for this installation by setting the variable called Local_Timezone. Valid values are UTC, GMT, ET, EST, EDT, CT, CST, CDT, MT, MST, MDT, PT, PST, PDT, or an ±hour[:min] offset from GMT such as “+9”. The ET, CT, MT, and PT versions auto-adjust for daylight saving time in these time zones (e.g., ET is

EDT between 2AM on the first Sunday in April and 2A.M. on the last Sunday in October; otherwise it is EST) and set the default timezone to standard time:

  - **`set Local_Timezone = "PT"`**

- SETTING DEBUG MODE: *eXpert-BSM* can operate in debug mode, under which it generates a console debug message for every BSM record it encounters. The settings for this variable are "off" (default) and "on" to produce event stream debug messages.

  - **`set DEBUG_MODE = "off"`**

- SETTING DELETION PROMPT FOR RESULTS DIRECTORY: You can specify whether `Run_eXpert_BSM` will prompt you to delete the current contents of the results directory. You can disable this check for non-interactive batch runs by setting this variable to "off"; "on" is the default.

  - **`set CLEAR_RES_DIR = "on"`**

- SETTING INVOCATION PROMPT FOR GUI: `Run_eXpert_BSM` can be configured to prompt the user for GUI invocation. This check can be disabled for non-interactive batch runs by setting this variable to "off"; "on" is the default.

  - **`set CHECK_GUI_INVOCATION = "on"`**

- ENABLING IPC TRANSPORT METHOD: IPC_METHOD tells eXpert-BSM that its components shall use Solaris sockets, unamed pipes, or shared memory. By default, sockets are used for communication between eXpert-BSM and ebsmgen.

  - **`set IPC_METHOD = "SOCKETS"`**

- EFUNNEL_MODE: Run_eXpert_BSM can be configured to forward its alerts to other subscriber EMERALD correlation, response, or visualization services located on remote servers. Connection establishment can be set to 1) filemode, indicating alerts should be sent to the local log file 2) passive , indicating eXpert-BSM should allow a subscriber running on the EFUNNEL_HOST to connect to it, or 3) initiate , indicating eXpert-BSM should connect into the subscriber on the EFUNNEL_HOST useful for firewall policies that may prevent eXpert-BSM from connecting out. Filemode is the default.

  - **`set EFUNNEL_MODE = "FILEMODE"`**

- EFUNNEL__HOST: If set, this is the host that eXpert-BSM will send its resolver alerts to if this function was enabled as described above. This parameter is commented out by default, causing Run_eXpert_BSM to prompt the user for the hostname. You can give either a hostname or an IP address.

  - **`set EFUNNEL_HOST = "consumer.your-domain.org"`**

Configuring the eXpert-BSM Knowledge-Base

eXpert-BSM provides parameters for customizing its knowledge-base for use in your environment. The parameters are accessible from **$Install/resource-object/-config/eXpert-config.inc**. The complete list of parameters that are available for knowledge-base custimization are provided below. At a minimum, the operator should closely consider the following parameter settings before using eXpert-BSM:

- EXPERT_ACTIVE_REPORTS_ENABLED
- BSM_ADMINISTRATOR_USER_LIST
- BSM_USER_HOMES_LOCATION
- BSM_LAST_RESERVED_ACCOUNT
- BSM_LOCAL_FTPD_UID
- BSM_FTP_UPLOAD_PATHS
- BSM_TCP_WRAPPER_LIST

Parameter: EXPERT_ACTIVE_REPORTS_ENABLED

- Dependent Rules: Status Message Generatrion
- Purpose: This flag enables the production of "I'm alive" status messages for use by EMERALD remote user interface software.
- Default: None. 0 (disabled)

```
Ulong EXPERT_ACTIVE_REPORTS_ENABLED 0
```

Parameter: BSM_ADMINISTRATIVE_USER_LIST

- Dependent Rules: BSM_Suspicious_Setuid, BSM_Illegal_Shadow_Passwd_Access, BSM_Promiscuous_Mode, BSM_Root_by_Nonadmin, BSM_Setreuid_by_Nonadmin
- Purpose: This list informs eX*pert-BSM* who the current list of users are that may legally acquire root control. Note: leaving this list empty effectively disables heuristics that depend on it.
- Default: None. root.

```
MsgString BSM_ADMINISTRATIVE_USER_LIST { root }
```

Parameter: BSM_MAX_BACKWARD_TIME

- Dependent Rules: BSM_TIME_Warp.
- Purpose: Indicates the number of seconds the host's time is allowed to be set backward before an alarm is raised.
- Default: 600 seconds (10 minutes)

```
Ulong  BSM_MAX_BACKWARD_TIME = 600
```

Parameter: BSM_SUSPICIOUS_EXEC_LIST

- Dependent Rules: BSM_SUSPICIOUS_EXEC_ARGUMENT
- Purpose: A list of highly suspicious program names that may be worthy of administrative review if executed on the host. The list can also be employed for site-specific surveillance needs.
- Default: A small set of well-known hacker programs.

```
MsgString BSM_SUSPICIOUS_EXEC_LIST  {
       perlmagic rootk ps_exp
       smurf pepsi nfsshell
       sniffer slammer satan
       nmap }
```

Parameter: BSM_EXEC_LESS_ACCOUNTS

- Dependent Rules: BSM_Special_User_Exec
- Purpose: A list of user accounts not intended to run processes. These accounts are present strictly for file ownership purposes. Other good candidates include ingress, uucp, nuucp, adm, listen.
- Default: bin, sys, noaccess

```
MsgString BSM_EXEC_LESS_ACCOUNTS {bin sys noaccess}
```

Parameter: BSM_USER_ENV_FILES

- Dependent Rules: BSM_Change_User_Environ_File

- Purpose: a list of environment initialization files that should not be modified by anyone other than the owner of the files. Other good candidate files include X server and mail configuration files.
- Default: .cshrc, .forward, .rhosts, .login, .logout, .profile, .tcshrc, .bach_login, .bash_profile

```
MsgString BSM_USER_ENV_FILES  {.cshrc .forward
.rhosts  .login .logout .profile .tcshrc .bash_login
.bash_profile}
```

Parameter: BSM_USER_HOMES_LOCATION

- Dependent Rules: BSM_Access_Private_File
- Purpose: The top directory under which user home directories are available from the host machine.
- Default: /homes/

```
Char BSM_USER_HOMES_LOCATION = /homes/
```

Parameter: BSM_EMERALD_NIC_NAMES

- Dependent Rules: BSM_PROMISCUOUS_MODE_ATTEMPT
- Purpose: The list of interfaces available on this machine. Use ifconfig -a to list the interface names.
- Default: hme0

```
MsgString BSM_EMERALD_NIC_NAMES   {hme0 }
```

Parameter: BSM_SYSTEM_BIN_LOCATIONS

- Dependent Rules: BSM_MOD_SYSTEM_EXECUTABLE
- Purpose: The list of directories under which system binaries are stored. Alterations of files from these locations are not allowed.
- Default: /bin/, /usr/bin/, /usr/local/bin/, /opt/local/bin/, /usr/sbin

```
MsgString BSM_SYSTEM_BIN_LOCATIONS  {
                                  /bin/
                                  /usr/bin/
                                  /usr/local/bin/
                                  /usr/sbin/
```

```
                                         /opt/local/bin/
                                           }
```

Parameter: BSM_SYSTEM_LOG_LOCATIONS

- Dependent Rules: BSM_MOD_SYSTEM_RESOURCES/BSM_SYSTEM_RESOURCE_FILES
- Purpose: The list of directories under which system logging files are stored. Alterations of the log files under these directories from non-authorized users in these locations are not allowed.
- Default: /var/log/, /var/adm/

```
MsgString BSM_SYSTEM_LOG_LOCATIONS {/var/log/   /var/adm/}
```

Parameter: BSM_SYSTEM_RESOURCE_FILES

- Dependent Rules: BSM_MOD_SYSTEM_RESOURCES/BSM_SYSTEM_RESOURCE_FILES
- Purpose: An explicit list of files within which security-relevant configuration parameters are stored. Alterations of files from non-authorized users in these locations are not allowed.
- Default: Selected configuration files.

```
MsgString BSM_SYSTEM_RESOURCE_FILES {
   /etc/group          /etc/hosts.equiv
   /etc/inittab        /etc/motd
   /etc/resolv.conf    /etc/netconfig
   /etc/nfssec.conf    /etc/printcap
   /etc/system         /etc/inetd.conf
   /etc/inet/inetd.conf /etc/printers.conf
   /etc/inet/ntp.conf  /etc/hosts.deny
   /etc/hosts.allow      /etc/nsswitch.conf
   /etc/defaultrouter  /etc/syslog.conf
   /etc/defaultdomain  /etc/resolv.conf
   /etc/hostname.hme0
}
```

Parameter: BSM_LAST_RESERVED_ACCOUNT

- Dependent Rules: BSM_MOD_SYSTEM_RESOURCES
- Purpose: Indicates the last priviledged UID present on the system. Unix systems, often by convention, will assign priviledged or other system accounts low number

UIDs (e.g., between 0 and 100). Such accounts include root, sys, bin, daemon, ftp, uucp, and lp. If the target host employs this convention, then assign to this variable the last system account ID. If not, set this value to the last UID (disable its use).

- Default: UID = 100

```
Ulong BSM_LAST_RESERVED_ACCOUNT =  100
```

Parameter: BSM_LOCAL_FTPD_UID

- Dependent Rules: BSM_FTP_Anon_Write, BSM_FTP_Warez_Activity
- Purpose: For environments in which a non-zero UID is employed for the ftpd system process.
- Default: UID = 0

```
Ulong BSM_LOCAL_FTPD_UID =  65533
```

Parameter: BSM_MAX_LOGIN_THRESHOLD

- Dependent Rules: BSM_Reach_Max_BadLogin
- Purpose: Indicates the number of bad logins that must occur during the FAILED_LOGIN_WINDOWS before a warning is raised for repeated failed log-ins.
- Default: 4

```
Ulong BSM_MAX_LOGIN_THRESHOLD =  4
```

Parameter: BSM_FAILED_LOGIN_WINDOW

- Dependent Rules: BSM_Reach_Max_BadLogin, BSM_FTP_Passwd_Guesser
- Purpose: Indicates the time window in which the failed logins must occur. That is, if N bad logins occur during S seconds (where N = BSM_MAX_LOGIN_THRESHOLD and S = BSM_FAILED_LOGIN_WINDOW), then a repeated failed login warning is raised.
- Default: 180 seconds (3 minutes)

```
Ulong BSM_FAILED_LOGIN_WINDOW =  180
```

Parameter: BSM_MAX_FTP_BADPASSWORDS

- Dependent Rules: BSM_FTP_Passwd_Guesser, BSM_FTP_Username_Guesser
- Purpose: Indicates the number of failed FTP login attempts that must occur before an alert is raised. This applies to failed FTP logins resulting from either bad usernames or bad passwords.
- Default: 4 bad usernames or passwords submitted to the ftp authentication service.

```
Ulong BSM_MAX_FTP_BADPASSWORDS =  4
```

Parameter: BSM_MAX_NOSPACE_ERRORS

- Dependent Rules: BSM_File_Exhaustion_Threshold
- Purpose: Indicates the number of repeated failed write attempts that must occur during the time window before a filesystem exhaustion alert is raised.
- Default: 8 file write or create failures due to no space errors per threshold cycle.

```
Ulong BSM_MAX_NOSPACE_ERRORS  =   8
```

Parameter: BSM_WRITE_ERR_THRESHOLD_WINDOW

- Dependent Rules: BSM_File_Exhaustion_Threshold
- Purpose: the time window, represented in seconds, during which repeated failed write attempts must occur.
- Default: 60 seconds

```
Ulong BSM_WRITE_ERR_THRESHOLD_WINDOW   =   60
```

Parameter: BSM_MAX_CLIENT_PROCS_PER_CYCLE

- Dependent Rules: BSM_Client_INET_Watch
- Purpose: Indicates the number of inetd connections that may occur during the time window. This heuristic is relevant for detecting process table exhaustion denial of service.
- Default: 8 connections

```
Ulong BSM_MAX_CLIENT_PROCS_PER_CYCLE =  8
```

Parameter: BSM_EXTERNAL_CONN_THRESHOLD_WINDOW

- Dependent Rules: BSM_Client_INET_Watch
- Purpose: The time window, represented in seconds, during which repeated inetd connections are measured.
- Default: 60 seconds

```
Ulong BSM_EXTERNAL_CONN_THRESHOLD_WINDOW =  60
```

Parameter: BSM_MAX_FAILED_PROCS_PER_CYCLE

- Dependent Rules: BSM_PROC_EXHAUST_THRESOLD
- Purpose: Indicates the number of failed forks observed by *eXpert-BSM* during the time window. This heuristic is relevant for detecting process table exhaustion denial of service.
- Default: 8 connections over 60-second period.

```
Ulong BSM_MAX_FAILED_PROCS_PER_CYCLE =  8
```

Parameter: BSM_MAX_FAILED_PROCS_THRESHOLD_WINDOW

- Dependent Rules: BSM_PROC_EXHAUST_THRESOLD
- Purpose: The time window, represented in seconds, during which repeated failed forks may be observed.
- Default: 60 seconds

```
Ulong BSM_FAILED_PROCS_THRESHOLD_WINDOW =  60
```

Parameter: BSM_MAX_ECHOS_RECEIVED

- Dependent Rules: BSM_Self_Echo_Flood
- Purpose: Indicates the number of local pings that must be observed during the time window before the self-ping denial-of-service alert is raised.
- Default: 30 echoes received in this cycle (see BSM_ECHO_FLOOD_WINDOW)

```
Ulong BSM_MAX_ECHOS_RECEIVED =  30
```

Parameter: BSM_ECHO_FLOOD_WINDOW

- Dependent Rules: BSM_Self_Echo_Flood
- Purpose: The time window, represented in seconds, during which repeated echo flood must occur.
- Default: 60 seconds

```
Ulong BSM_ECHO_FLOOD_WINDOW  =  60
```

Parameter: BSM_UNACCEPTABLE_PORT_CONNECTS

- Dependent Rules: BSM_Alert_On_Port
- Purpose: List of TCP ports to which external clients should not connect.
- Default: ports 53 (dns), 143 (imap), 514 syslog

```
Ulong BSM_UNACCEPTABLE_PORT_CONNECTIONS {53  143  514}
```

Parameter: BSM_NONADMIN_EXPIRE

- Dependent Rules: BSM_Root_By_Nonadmin
- Purpose: Once an alert is raised indicating that a non-administrative user is operating as an administrator, *eXpert-BSM* suppresses repeated alerts of this condition for a duration of BSM_NONADMIN_EXPIRE seconds.
- Default: 600 seconds, 10 minutes

```
Ulong BSM_NONADMIN_EXPIRE =  600
```

Parameter: BSM_FTP_WAREZ_COMPLAINT

- Dependent Rules: BSM_FTP_Warez_Activity
- Purpose: In some environments an external anonymous user may be permitted to upload a file. This capability is subject to several abuses, including the potential for turning the target host into a warez site. This variable specifies the number of times an anonymously uploaded file can be **downloaded** by other external ftp clients.
- Default: 5

```
Ulong BSM_FTP_WAREZ_COMPLAINT =  5
```

Parameter: BSM_ANON_FILE_EXPIRE

- Dependent Rules: BSM_FTP_Warez_Activity
- Purpose: Indicates the amount of time *eXpert-BSM* will remember a file written by an anonymous ftp user. During this period, if there is a subsequent flood of anonymous external reads of this file, an alert is raised of potential warez client activity.
- Default: 259200 seconds, or 72 hours

```
Ulong BSM_ANON_FILE_EXPIRE =  259200
```

Parameter: BSM_FTP_UPLOAD_PATHS

- Dependent Rules: BSM_FTP_Anon_Write
- Purpose: Indicates the directory path under which anonymous ftp writes are allowed.
- Default: /pub/ftp/incoming

```
MsgString BSM_FTP_UPLOAD_PATHS
        {
                /pub/ftp/incoming
        }
```

Parameter: BSM_TCP_WRAPPER_LIST

- Dependent Rules: BSM_Inetd_Subversion
- Purpose: Indicates the full pathname of any and all TCP wrapper binaries employed by Inetd services.
- Default: empty list

```
MsgString BSM_TCP_WRAPPER_LIST
        {
        }
```

Parameter: BSM_ENABLED_HEURISTICS

- Dependent Rules: All

  Purpose: Indicates the list of active heuristics enabled within the knowledge-base. By removing an entry, you effectively disable the rule upon the next initialization of *eXpert-BSM*. Heuristics: BSM_Time_Warp, BSM_Root_Core_Creat, BSM_Reach_Max_BadLogin, BSM_Root_Core_Event, BSM_FTP_Passwd_Guesser, BSM_FTP_Username_Guesser, BSM_PS_Exploit, BSM_Suspicious_Exec_Argument, BSM_Root_Core_Access, BSM_Access_Private_File, BSM_Make_Temp_Sym, BSM_Mod_System_Resource, BSM_FTP_Anon_Write, BSM_FTP_Warez_Activity, BSM_Setreuid_By_Nonadmin, BSM_Proc_Exhaust_Threshold, BSM_Client_INET_Watch, BSM_File_Exhaust_Threshold, BSM_Attempted Root_Login, BSM_Suspicious_Setuid, BSM_Port_Sweep, BSM_Suspicious_Port_Probing, BSM_Bad_Port_Connection, BSM_AfterHours_Access, BSM_Buffer_Overflow_Exec, BSM_Special_User_Exec, BSM_Exec_Non_Author, BSM_Change_User_Environ_File, BSM_Self_Echo_Alert, BSM_Illegal_Shadow_Passwd_Access, BSM_Root_By_NonAdmin, BSM_Disallowed_File_Read, BSM_Disallowed_File_Exec, BSM_Disallowed_File_Write, BSM_Promiscuous_Mode, BSM_Mod_System_Executable, BSM_Inetd_Subversion

- Default: All rules enabled

```
MsgString BSM_ENABLED_HEURISTICS
 {
  BSM_Time_Warp
  BSM_Root_Core_Creat
  BSM_Reach_Max_BadLogin
  BSM_Root_Core_Event
  BSM_FTP_Passwd_Guesser
  BSM_FTP_Username_Guesser
  BSM_Suspicious_Exec_Argument
  BSM_AfterHours_Access
  BSM_Root_Core_Access
  BSM_Access_Private_File
  BSM_Mod_System_Resource
  BSM_FTP_Anon_Write
  BSM_FTP_Warez_Activity
  BSM_Setreuid_By_Nonadmin
  BSM_Client_INET_Watch
  BSM_Proc_Exhaust_Threshold
  BSM_File_Exhaust_Threshold
  BSM_Attempted Root_Login
  BSM_Suspicious_Setuid
  BSM_Port_Sweep
  BSM_Suspicious_Port_Probing
  BSM_Bad_Port_Connection
  BSM_PS_Exploit
  BSM_Buffer_Overflow_Exec
  BSM_Special_User_Exec
  BSM_Exec_Non_Author
  BSM_Change_User_Environ_File
  BSM_Illegal_Shadow_Passwd_Access
  BSM_Mod_System_Executable
```

```
        BSM_Root_By_NonAdmin
        BSM_Disallowed_File_Read
        BSM_Disallowed_File_Exec
        BSM_Disallowed_File_Write
        BSM_Promiscuous_Mode
        BSM_Self_Echo_Alert
        BSM_Inetd_Subversion
      }
```

Configuring the Local Network Address List

eXpert-BSM maintains a local IP address list that is used to distinguish internal from external port connections in those heuristics that deal with network connections. The local network IP address list is located in:

`$Install/resource_object/config/local_netmap.conf`.

It should enumerate the list of IP addresses that are considered local to your administrative domain. These IP addresses can be enumerated in either of two ways: by subnet mask or by specific IP address.

```
syntax:
       net <network address[/network-bits]>
or
       host <ip_address or fully qualified hostname>
```

The optional network-bits field indicates how many of the most significant bits in the network address are considered to be the network or subnet while the rest of the bits denote the host.

The file can contain any number of net and host entries. The following is an example of specifications of addresses in the `local_netmap.conf` file:

```
net   172.16.0.0
net   190.80.20.0/24
host  192.168.1.1
host  myhost.mydomain.com
```

The above entry will inform *eXpert-BSM* that hosts from the class B network 172.16.*.*, subnet 190.80.20.*, host 192.168.1.1, and host `myhost.mydomain.com` are local to the administrative domain of the *eXpert-BSM* host machine.

Configuring the Surveillance Policy for Local File Access

eXpert-BSM provides a facility for specifying a surveillance policy over file reads, writes, and executions. Under this policy, you may specify groups of users and files or directories, and then use these groups to specify surveillance policies regarding file accesses.

Please note that this is a *surveillance* policy that is used to warn about access violations; *eXpert-BSM* is a passive monitor that cannot prevent the access violations from taking place.

There are three distinct components to be specified within an *eXpert-BSM* access policy specification. The first, the `UserGroups {}` section, allows you to specify groups of users, which are then referenced in the access policy. The `UserGroups {}` section is specified as follows:

```
UserGroups   {
               user_list_1 {user1a  user1b ...}
               user_list_2 {user2a  user2b ...}
               ...
             }
```

The names specified under the user groups should be present as valid login names defined within the password file, and user names can appear in multiple lists.

The second section, `FileGroups {}`, allows you to specify a set of files and directories that may be referenced together as a group while enumerating the access policy. The `FileGroups {}` section is specified as follows:

```
FileGroups {
             file_list_1{file1a file1a ... directory1a ...}
             file_list_2{file1a file1a ... directory1a ...}
             ...
           }
```

Files specified in the file groups should be fully qualified pathnames. You can also specify directories, as shown below in the example access policy specification. Files and directories can appear in multiple lists.

The third section is `Policy {}`, within which you specify illegal read, write, and execute accesses between users and files. The `Policy {}` section is specified as follows:

```
Policy    {
       user_list_1{
               nread [ file_list_1 file_list_2 ... ]
               nwrite[ file_list_3 file_list_4 ... ]
               nexec [ file_list_5 file_list_6 ... ]
       }
       user_list_2{
               nread [ file_list_1 file_list_2 ... ]
               nwrite[ file_list_3 file_list_4 ... ]
               nexec [ file_list_5 file_list_6 ... ]
       }
       ...
}
```

The policy involves a series of relations defined between user and file groups. For each user group entered in the policy, three possible relations can be specified: `nread,` `nwrite`, and `nexec.` `nread` indicates that users in the associated list are not allowed to read files matching the file lists specified in the bracket clause. Illegal file writes and executions are specified similarly. It is not necessary for every relation to be specified in the user list, and file lists may be empty, indicating no defined restrictions.

The following is an example EMERALD access policy specification:

```
UserGroups { RegStaff   (em_user1 em_user2)
             Management (em_admin )
             Accnt      (em_acct)
}
FileGroups { Programs ( /bin /usr/bin
                        /usr/local/bin
                        /usr/local/ftp/bin )
             Admtools ( /etc/bin /etc/sbin
                        /usr/sbin /sbin )
             CompanySecrets  ( /secret )
             Payroll  ( /accounting/DBMS/payroll.db )
}
Policy {
             RegStaff (
                   nread[CompanySecrets Payroll]
                   nwrite[CompanySecrets Programs Payroll
                          Admtools]
                   nexec[Admtools] )
             Management(
                   nread[]
                   nwrite[Programs Admtools]
                   nexec[] )
             Accnt (
                   nwrite[Programs Admtools]
                   nread[CompanySecrets]
                   nexec[Admtools] )
}
```

In the above example, which illustrates a valid access policy specification, there exists a small group of regular staff defined as `em_user1` and `em_user2`. There is a management staff, with one manager `em_admin` and an accounting group consisting of user `em_acct`. Four file groups are defined. The first is the programs group, where programs are defined as being located in `/bin, /usr/bin/, /usr/local/bin/,` and /usr/local/ftp/bin. An administrative tools bin consists of files in /etc/bin, /etc/sbin, /usr/sbin, and /sbin. A directory containing company secrets is named /secret. A payroll file group consists of a file called /accounting/DBMS/payroll.db.

The access policy is now ready to be specified. In the example, regular staff are not allowed to read company secrets or payroll data, as specified by the associated nread function. Regular staff may not write to files in the company secrets, programs, payroll, or admin tools. Further, regular staff may not execute admin tools. If *eXpert-BSM* observes user activity that contradicts this policy, an alert is raised. Management staff is not allowed to modify files in the program or admin tools file groups, but have unrestricted read and execute access over the entire system. Members of the accounting staff are not allowed to modify files in the program or admin file groups, read company secret files, or execute admin tools.

Dynamically Adjusting eXpert-BSM's Configuration

Modifications to the configuration parameters specified in eXpert-Config.inc, username.map, accesspolicy.conf, and local_netmap.conf, can be dynamically recognized without restarting *eXpert-BSM*. To do this, perform a SIGHUP (see *kill(1)* for more information on sending SIGHUP signals to processes) on the running *eXpert-BSM*, and all parameters in these files will be reloaded from the disk.

Using the Configuration GUI to Set Parameters

eXpert-BSM provides a Java-based configuration management interface for setting the values of runtime parameters. This interface may be invoked directly from the *eXpert-BSM* installation program or it may be invoked at any time using the Run_config script.

11 Operating Instructions

eXpert-BSM can be invoked in three operating modes as follows:

```
$Install/_BSM/Run_eXpert_BSM

Usage:  Run_eXpert_BSM [ -TEST ]
         or Run_eXpert_BSM [ bsm_file ]
         Modes:
               REALTIME  - no arguments
               TEST      - optional -TEST directive invokes

                           eXpert-BSM against attack
                           battery located in

                           $Install/samples/attack-battery.ebin

               BATCH     - optional <bsm_file> provided
```

Real-time: The advantage of running eXpert-BSM with direct kernel record capture is that it significantly reduces the overhead of secondary storage write and read operations, as well as the expense of secondary-storage to maintain a permanent audit file. Instead, eXpert-BSM reads audit records directly from the kernel and alerts about those records representing malicious activity. To begin analysis, move to the eXpert-BSM run directory (`$Install/_BSM`) and execute the following command:

```
% Run_eXpert_BSM
```

Test Mode: *eXpert-BSM* can be directed to process an EMERALD-encoded binary audit file to test and illustrate the effectiveness and reporting structure of this component. The binary file `$Install/samples/emerald-attack-battery.ebin` will automatically be accessed when the TEST flag is set:

```
% Run_eXpert_BSM  -TEST
```

Batch-Mode Post-processing of Solaris Audit Files: *eXpert-BSM* can be targeted to an arbitrary BSM audit file. To begin analysis, move to the *eXpert-BSM* run directory (`$Install/_BSM`) and execute the following command

`% Run_eXpert_BSM` <*BSM_Audit_File*>

Security Daemon Mode (autoboot operation): The Solaris operating system can be configured to automatically start eXpert-BSM as part of its initialization procedures. This capability is done by inserting the script in the `/etc/init.d/expert-BSM`, and creating a symbolic link `/etc/rc2.d/S80eXpert-BSM` to that shell script. If you would like to alter the startup ordering position of eXpert-BSM you can do so by altering the name of the symbolic link. We recommend that if you would like to temporarily disable eXpert-BSM, you do so by modifying the name of the symbolic link to `/etc/rc2.d/disabled-S80eXpert-BSM`. To reinsert eXpert-BSM into the Solaris Startup procedure, simply restore the name of the symbolic link.

In Security daemon mode, all eXpert-BSM alert logs are stored in directory /var/adm/securityd/. During the startup and shutdown process, syslog entries are provided as facility type daemon and severity level notice, and allow the user to determine the state of eXpert-BSM. The following syslog entries are possible:

`Solaris security daemon mode...started` – eXpert-BSM has been successfully started.

`Solaris security daemon mode...shutdown` – `eXpert-BSM has successfully shutdown.`

`securityd error...missing argument` – a problem has occurred in with the /etc/init.d/eXpert-BSM script. Please try re-running Install_eXpert_BSM.

`securityd path not located` – Perhaps the eXpert-BSM installation directory has been moved or is no longer available. Please locate the eXpert-BSM installation directory and rerun `Install_eXpert_BSM`.

`securityd cannot run with auditd` - eXpert-BSM determines whether the audit daemon is currently set to start at boot time on your system. This should not be the case if you want to run in real-time; as eXpert-BSM real-time mode does not work in parallel with the Solaris audit daemon. Auditd should have been deleted as part of the installation procedure. Please rerun the installation script.

`securityd directories unavailable` – Perhaps the eXpert-BSM installation directory has been moved or is no longer available, or a key configuration file is missing. Please locate the eXpert-BSM installation directory and rerun `Install_eXpert_BSM`. If that doesn't work, reinstall the eXpert-BSM package.

`securityd resource object not available` – Please locate the eXpert-BSM installation directory and rerun `Install_eXpert_BSM`. If that doesn't work, reinstall the eXpert-BSM package.

`securityd results directory unavailable` – directory `/var/adm/securityd/` does not exist and eXpert-BSM could not create the directory.

`securityd EFUNNEL_HOST undefined` – variable EFUNNEL_HOST in `$INSTALL/_BSM/eXpert-config.sh` references a host that is unreachable by eXpert-BSM. Disable alert forwarding, or reassign the target hostname.

`securityd access map not found` – eXpert-BSM could not find file $INSTALL/resource-obect/config/accesspolicy.conf. This is not a required file.

`securityd alerts are forwarding to <EFUNNEL_HOST>` – eXpert-BSM has successfully connected to the efunnel host target and will send intrusion alerts to that machine.

`securityd alerts are availble in <results file>` – eXpert-BSM will send intrusion alerts to the named results file.

`securityd stop path not located` – Perhaps the eXpert-BSM installation directory has been moved or is no longer available. Please locate the eXpert-BSM installation directory and rerun `Install_eXpert_BSM`.

The eXpert-BSM Process Chain

`Run_eXpert_BSM` is a csh script that invokes the following programs

- `ebsmsetpolicy` - (real-time mode) establishes an optimized audit policy configuration with the kernel. This utility needs to be setuid root and is therefore not distributed as a shell script. It exits immediately after setting the audit configuration.
- `ebsmprobe` - (real-time mode) establishes process-to-process communication between the Solaris kernel and ebsmgen. This is a setuid application. Proper shutdown of *eXpert-BSM* requires this utility to be terminated first, by either a SIGTERM or SIGHUP signal.
- `throttle` - (real-time mode) is an intermediate message utility to handle safe buffering between the kernel and ebsmgen. Always terminate ebsmprobe before terminating this application, otherwise the kernel may enter an unstable state as it fills its internal audit record queues.
- `ebsmgen` - (all modes) accepts Solaris BSM audit records, and converts and forwards them as EMERALD messages to *eXpert-BSM.*
- `eXpert-BSM` - (all modes) is the EMERALD forward-chaining expert system.

12 Shutdown Instructions

Login under the account that started *eXpert-BSM* (or root) and invoke

```
  $Install/_BSM> Shutdown_eXpert_BSM
```

This script kills the process chain for the eXpert-BSM. In real-time mode, this script kills ebsmprobe, throttle, ebsmgen, and eXpert-BSM in that order.

CAUTION: When running in real-time mode do not attempt to kill the process throttle "by hand" before shutting down ebsmprobe. Doing so will cause system instability.

Note: If several start-stop runs are made, the output will accumulate in the results directory (i.e., the results of each run **do not** overwrite the previous results, but you could tell the run script to clear the results directory before starting a new run). You may delete any old (i.e., *.log, *.resolver, or *.ascii) results at any time, as long as they are not the output of a currently running monitor.

Autoboot Shutdown

When running in autoboot mode, *eXpert-BSM* can be manually terminated by the following command:

```
      $Install/_BSM> /etc/init.d/eXpert-BSM stop
```

13 Uninstalling *eXpert-BSM*

The eX*pert-BSM* monitor can be safely uninstalled as follows:

1. If eX*pert-BSM* is currently running, shut it down before attempting to uninstall this component.

2. Remove the eX*pert-BSM* install directory.

3. If you want to restore the original BSM audit configuration of the host, as root move to directory /etc/security and untar file `/etc/security/orig_audit_file{install timestamp}.tar.gz`.

4. If you would like to disable the audit capability of the system, you could follow the procedure in Solaris Audit Installation but use the `bsmunconv` script instead of `bsmconv`.

5. If you have configured *eXpert-BSM* for autoboot mode, the following files and directories should be removed: `/etc/init.d/expert-BSM`, `/etc/rc2.d/S80eXpert-BSM`, `/var/adm/securityd/`

14 *eXpert-BSM* Report Formats

The EMERALD eX*pert-BSM* monitor produces three forms of intrusion reports: console alert, EMERALD resolver alerts, and IDIP alerts.

Console Alert Format

eXpert-BSM produces attack alerts, which by default are placed in

```
        $Install/_BSM/results/bsm-expert-{timestamp}.log
```

The console alert format is structured as follows.

```
0.  ------------------------------------------------------------
1.  (RepID|ThreadID) <Severity> <rule> Target: <> Count: <>;
2.       Observer: <>;   Observer_location: <>;  Observer_src: <>
3.       Start_time: <>  End_time: <>
4.       Command: <>     Parent_cmd: <>   Outcome = <>
5.       Attacker: <>
6.       Attacker_attrs: <attribute list>
7.       Command_arg: <>
8.       Resource: <>  Resource_owner: <>
9.       Recommendation: <>
10.      Comment: <>
```

Console alerts contain a maximum of 10 lines. Lines 6-10 are optional.

Line 1: provides a summary of the key attributes of the attack. The `RepID` is a unique identifier for this alert (its value is derived from the event count of the audit record under which the alert was generated). In addition, a `ThreadID` is provided which is used to associate the alert with a previous report. The `ThreadID` is usually equal to the `RepID`, unless the report is a "follow-on" with additional information from a previously written report. In that case, the `ThreadID` equals the `RepID` of the preceding associated alert. The `Severity` field indicates the type of alert this report represents (Debug, Informative, Warning, Severe_Warning, Attack. These values are defined as follows:

DEBUG_INFO	Optional console message only for event stream debugging and low-priority messages.
INFORMATIVE	Optional low-priority messages on monitor status.
WARNING	Exceptional activity that is symptomatic of possible system distress or security-relevant operations. The accumulation of WARNING level alerts is worthy of administrative review.
SEVERE_WARNING	Activity that maps to known intrusive activity. Other nonmalicious explanations are possible.

ATTACK	Indicates activity maps to known intrusive activity. Nonmaliciously produced occurrences of this activity are rare or non-existent

Next, the `rule` represents the name of the rule that has fired, which may be potentially useful for tuning rules should the user not desire some alerts. The `Target` field indicates the hostname of the machine, and the `Count` field indicates the number of times the malicious activity is observed for this report.

Line 2: indicates the name of the sensor that produced the alert; in this case the `observer` is eXpert-BSM. In addition, the `observer_location` represents the IP address of the host on which observer is run, and `observer_src` indicates whether the sensor is operating in real-time or batch mode. If batch-mode, the BSM filename is provided.

Line 3: provides the `Start_time` and `End_time` of the attack. The `Start_time` is mandatory, and represents the timestamp relative to the event stream, at which the malicious activity is observed. The `End_time` is optional, and used only for intrusion reports that span a duration.

Line 4: provides the name of the operation that is being performed. With respect to BSM, this represents the system call name or high-level audit event name provided by the BSM audit trail of the key record used to distinguish the attack. The `Parent_cmd` is a synthetically generated string derived by tracing the process within the audit stream. For example, if the file `/bin/rm` is invoked such that *eXpert-BSM* reports an illegal unlink(2) operation, the command reported by the alert is `unlink`, and the `Parent_cmd` will be `/bin/rm`. The `Outcome` reports the audit return value on a given operation. Interpretation of this field is operation dependent.

Line 5: indicates the identity of the attacker. If at all possible, this represents the username of the individual responsible for the attack. For network-related attacks, this represents the remote IP address of the attacking host.

Line 6: (optional) provides an alert-dependent enumeration of supportive information.

Line 7: (optional) where applicable provides additional information regarding the arguments used to invoke an operation. With respect to BSM analysis, the `Command_arg` field is used to represent the exec_args parameter with respect to process executions.

Line 8: (optional) where applicable, this line provides additional information regarding resources (usually files) that are manipulated during the malicious activity, and the owner of the object.

Line 9: (optional) provides recommended countermeasure directives for responding to intrusive activities. eXpert-BSM employs

- `KILL|KILL_ALL <session_id> ---` terminate the intrusive session (e.g., kill -9 <session_id>).
- `LOCKOUT <username> ---` disable the user account until the individual responsible for the malicious activity associated with this account is found.
- `FIXPERMS <filename> ---` alter the target file access permissions as specified.
- `FILTER <IP address> ---` if a firewall is available, disallow network connectivity from this indicated IP address.
- CHECKCFG <Host> <Service> `--- identifies system service that appears to have been attacked or has died.`
- `DIAGNOSE <Network Service | Filesystem> ---` Validate the correct operation of the named network service, or the availability of the named filesystem.

Line 10: (optional) The primary use of this line is to indicate the relevant user configuration parameters that modify the behavior of the rule that generated this alert.

EMERALD Resolver alerts

The EMERALD resolver alerts are by default written to

```
    $Install/_BSM/results/bsm-alert-{timestamp}.resolver
```

but could also be sent to another EMERALD components such as the alert collection application *efunnel* or an analysis engine on a higher level. Resolver alerts can be displayed by the graphical EMERALD Alert Management Interface described in the following section.

Alert Management Interface

EMERALD provides a unique graphical user interface for managing alerts produced by EMERALD sensors. Using this interface, you can view individual alerts, manage incident handling reports, print reports, forward reports via email, and view recommendations on responding to attacks. For more information on the Alert Management Interface, refer to the EMERALD Alert Management Interface User's Guide, Version 1.2 (available in `$Install/doc/Emerald-AMI-1-2-manual.pdf`).

15 *eXpert-BSM* Testing

EMERALD provides an extensive test suite of attacks to exercise its host-IDS knowledge base. The attack battery is an EMERALD-encoded Solaris BSM data set that can be invoked directly from the `Run_eXpert_BSM` script:

```
% Run_eXpert_BSM -TEST
```

A full test description of the EMERALD host-based attack battery is available in Appendix I. The console alerts produced from the EMERALD host-based attack battery are available for review in Appendix II.

Remember that when testing eXpert-BSM in real-time mode, you must ensure that the session you are mounting test attacks from is not the same session under which you initialized eXpert-BSM (i.e., to initiate a new session, log completely out of the target host).

The use of network-based vulnerability scanners has become a prominent practice in security evaluation procedures. An evaluator pointing a scanner, such as one of the popular commercial or free network-based vulnerability scanners, against a host system with a host-based intrusion detection system such as eXpert-BSM is likely to be disappointed when eXpert-BSM does not react to all elements of the scan.

16 Caveats and Known Bugs

For the latest set of caveats, known bugs, and frequently asked questions, visit our current Release Notes, at

http://www.sdl.sri.com/emerald/releases/eXpert-BSM/Release_Notes.html

For the list of Frequently Asked Questions regarding *eXpert-BSM*, visit

http://www.sdl.sri.com/emerald/releases/expert-BSM/faq.html

17 Version Status

EMERALD eX*pert-BSM*, Version 1.5, April 2002. See the EMERALD software distribution web page http://www.sdl.sri.com/emerald/releases for further information regarding our follow-on release that will precede the expiration of this release.

18 Credits and Acknowledgements

EMERALD Development Team
emerald@sdl.sri.com

Martin Fong, Ulf Lindqvist (PI), Phillip Porras (PD), Keith Skinner, Alfonso Valdes (PI), Peter Neumann, Sandy Smith, Steven Cheung, John Khouri, Kenneth Nitz, Magnus Almgren

EMERALD Development Project

August 1996 to April 2002

Acknowledgments:

DARPA Information Technology Office
DARPA Information Systems Office
National Security Agency

19 License, Feedback, & Contact Information

This Section describes the license and distribution terms for the release of eXpert-BSM evaluation edition. See the EMERALD software distribution web page http://www.sdl.sri.com/emerald/releases/ for further information regarding follow-on releases. See the end of this Section, Contact and Experience Reporting Information, for pointers on where to send questions, bug reports, and detected attack summaries.

Your responsibilities as an EMERALD eXpert-BSM User

There is no charge to use this application. Support for this evaluation edition is very limited in that the EMERALD team is not able to provide individual support. However, technical support is provided to licensees of the advanced version of eXpert-BSM, called eXpert-BSM Enterprise Edition, which is directly available for licensing from SRI International (contact emerald@sdl.sri.com for pricing information and licensing conditions).

By agreeing to the online version of the Software Distribution Agreement and downloading and using eXpert-BSM evaluation edition, you have agreed to the following terms and conditions:

- You will adhere to the Software Distribution Agreement below.
- You will adhere to the Reporting and Feedback Agreement below.

Software Distribution Agreement

U.S.A. Government Purpose Rights

Contract No.: F30602-96-C-0294
Contractor Name: SRI International
Contractor Address: 333 Ravenswood Ave.

The Government's rights to use, modify, reproduce, release, perform, display, or disclose this software are restricted by paragraph (b)(2) of the Rights in Noncommercial Computer Software and NonCommercial Computer Software Documentation clause contained in the above identified contract. Any reproduction of this software or portions thereof marked with this legend must also reproduce the markings.

Non-U.S.A.-Government Use Rights

THE FOLLOWING IS A LICENSE AGREEMENT RELATING TO THE ACCOMPANYING SOFTWARE. CAREFULLY READ ALL OF THE AGREEMENT'S TERMS AND CONDITIONS BEFORE PROCEEDING. IF YOU DO NOT AGREE TO SUCH TERMS AND CONDITIONS AND INDICATE YOUR ACCEPTANCE BELOW, YOU WILL NOT BE PERMITTED TO USE THE SOFTWARE.

By having clicked the YES box on the eXpert-BSM evaluation edition registration and download page of SRI’s website, you have agreed to the following provisions as a condition precedent to your possession and use of eXpert-BSM, an evaluation version software program for a Solaris Host-Based Intrusion Detection System (the “Program”) from SRI International (“SRI”), pursuant to the California Uniform Electronic Transactions Act.

1. Authority. You represent that you are either acting as an individual person on your own behalf or that you are acting on behalf of your employer and are authorized to accept these terms and conditions on its behalf (in either case hereinafter referred to as “you”). You agree that you have read and understand this Agreement.

2. Copyright. This Program is owned by SRI and is protected by United States copyright laws and international treaty provisions. Therefore, you must treat the Program like any other copyrighted material.

3. Grant of License. SRI hereby grants to you a nontransferable and nonexclusive license to possess and use the Program in accordance with the terms and conditions of this Agreement. The license authorizes you to use the Program on one computer or network system and SOLELY for your personal use and evaluation. You agree that you are licensing the Program for its end use only and not for resale or redistribution.

3.1 This license authorizes you to use the Program solely in accordance with this Agreement. You shall not sell, lease, assign, transfer, sub license, disseminate, modify, translate, duplicate, reproduce or copy the Program (or permit any of the foregoing) or disclose the Program or any information pertaining thereto any other party without the prior written consent of SRI.

3.2 You may not reverse-assemble or reverse-compile or otherwise attempt to create the source code from the Program.

4. Confidentiality. You acknowledge that the Program, including the related documentation and any new releases, modifications and enhancements thereto, belongs to SRI, and that SRI retains all right, title and interest in and to the Program. You further acknowledge that the Program and information relating thereto constitute valuable trade secrets of SRI. You agree to comply with the terms and conditions of this Agreement and agree to treat the Program as the confidential and proprietary information of SRI.

5. Disclaimer of Warranty. This Program is pre-release code and as such may not operate correctly and may be substantially modified prior to first commercial release. SRI does not guarantee service results or represent or warrant that the Program will be completely error-free. The Program is provided by SRI "AS IS".

5.1 SRI HEREBY DISCLAIMS ALL WARRANTIES OF ANY NATURE, EXPRESS, IMPLIED OR OTHERWISE, OR ARISING FROM TRADE OR CUSTOM, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE.

5.2 SRI SHALL NOT BE LIABLE FOR DAMAGES OF ANY KIND, INCLUDING GENERAL DIRECT, SPECIAL, INCIDENTAL AND CONSE-QUENTIAL DAMAGES, RESULTING FROM OR ARISING OUT OF THIS AGREEMENT OR YOUR USE OF THE PROGRAM.

6. Indemnity. You shall be solely responsible for the supervision, management and control of your use of the Program and any related products and documentation. You hereby indemnify and hold harmless SRI and its affiliates (the "Indemnified Parties") against any loss, liability, damages, costs or expenses suffered or incurred by the Indemnified Parties at any time as a result of any claim, action or proceeding arising out of or relating to your use, operation or implementation of the Program. For purposes of this Agreement, affiliate means any Company division or subsidiary or any other entity involved in the manufacture of the Program.

The Indemnified Parties shall not be responsible, and you shall have no recourse against the Indemnified Parties, for any loss, liability, damages, costs or expenses which may be suffered or incurred at any time by you as a result of your reliance upon or use of the Program, or as a result of any claim, action or proceeding against you arising out of or relating to the use of the Program, or as a result of your defense of any such claim, action or proceeding.

7. Term and Termination. Your license term is for a period of the lesser of one hundred and eighty (180) days after downloading the Program or until **January 31, 2003**. Subsequent one hundred and eighty (180) day periods under this license may be granted at SRI's sole discretion through your use of your assigned password (see web page instructions), in which event the terms and conditions of this license agreement shall remain in full force and effect. SRI may otherwise immediately terminate this license upon notice to you, whereupon you shall immediately destroy all copies of the Program. Upon the natural expiration of the initial license period of this agreement, the Program will automatically cease to function.

8. Reporting. At least once during the license term you shall report back to SRI your experiences with the use of the Program (see Contact and Experience Reporting Section below for feedback address).

9. Applicable Law. This Agreement and any disputes arising hereunder shall be governed by the laws of the state of California, United States of America, without regard to conflicts of laws principles. The parties hereby expressly exclude the application of the U.N. Convention on Contracts for the International Sale of Goods to the Agreement.

Reporting and Feedback Agreement

EMERALD eXpert-BSM is made available for your use in the spirit of free software evaluation and for the improvement of security across all computing environments. As a downloader and user of this software, you agree to the following terms and conditions:

1. Tell us your experiences using this software. Let us know if eXpert-BSM leads to the detection of any security compromises in your site. If so, please tell us which alert name(s) succeeded in providing useful detections. Tell us if, in your environment, any rules are encountered which repeatedly misfire on what you consider to be normal operating functions.
2. Tell us of any suggestions you may have in additional attack heuristics that you would like us to incorporate in future versions of eXpert-BSM
3. Tell us of any documentation errors, script failures, or system errors that you experience while using eXpert-BSM.

See Contact and Experience Reporting Information for information on how to submit feedback and bug reports.

Contact and Experience Reporting Information

If you experience problems or locate a problem in eXpert-BSM, please inform us using our address emerald-release@sdl.sri.com. We will do our best to incorporate fixes to your problems in the next release of EMERALD eXpert-BSM. We regret that individual end user support is not possible in this evaluation edition release. For other questions regarding the EMERALD program and the availability of other specialized security tools, you may contact the EMERALD Program Director, Phil Porras, at porras@sdl.sri.com.

For users requiring technical support for eXpert-BSM evaluation edition, direct all questions regarding special arrangement support agreements and licensing conditions to emerald-support@sdl.sri.com.

Please direct all experience reporting and feedback discussed in the Reporting and Feedback Agreement to emerald-feedback@sdl.sri.com.

Appendix I: Attack Battery Test Data Description

This document describes the 33 attack tests used for the EMERALD eXpert-BSM self-test attack battery.

Test 1: Buffer overflow in ps (BSM_PS_EXPLOIT)

Run the appropriate exploit program (or use LL data, uid 2053).

```
     Start_time: 1998-07-29 19:27:29.562456 EDT
     Command: execve(2)   Parent_cmd: /usr/bin/ps   Outcome: 0
     Attacker_attrs: auid= 2053 ruid= 2053 euid= 0 pid= 5593 sid=
5584
     Command_arg: ps
     Resource: /usr/bin/ps   Resource_owner: root
```

Test 2: Selfping (BSM_SELF_ECHO_ALERT)

```
    Start_time: 1999-04-05 20:17:10.001999 EDT
    End_time: 1999-04-05 20:18:09.992008 EDT
    Command: echo   Parent_cmd: inetd   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: auid= 2037 ruid= 0 euid= 0 pid= 24892 sid=
24802
    Recommendation: KILL 24802
    Comment: relevant params: BSM_MAX_ECHOS_RECEIVED,

             BSM_ECHO_FLOOD_WINDOW
```

Test 3: General buffer overflow (except ps) (BSM_BUFFER_OVERFLOW_EXEC)

Run the eject exploit program, renamed to something non-suspicious.

```
 Time:  1999-12-30 19:08:13.371242 EST
 UserName : admin_u  EffectiveName:   root  AuditName: admin_u
 RUID: 2037   EUID: 0   AUID: 2037   PID: 25345
```

Test 4: Known attack name (BSM_SUSPICIOUS_EXEC_ARGUMENT)

Run a phony program (such as an empty script) where the program name contains any of the forbidden words in BSM_SUSPICIOUS_EXEC_LIST.

```
 Time:  1999-12-30 19:08:51.011335 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25346
 Path List: [ /usr/bin/anyexploitany ]

 Time:  1999-12-30 19:08:51.011335 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25346
 Path List: [ /usr/emerald/em_user1/anyexploitany ]
```

Test 5: Special User Executes Program (BSM_SPECIAL_USER_EXEC)

As em_admin, su to root, then su to one of BSM_EXEC_LESS_ACCOUNTS, for example 'bin' and run 'ls'.

```
 Time:  1999-12-30 19:09:27.631431 EST
 UserName : bin  EffectiveName:   bin  AuditName: admin_u
 RUID: 2   EUID: 2   AUID: 2037   PID: 25350
 Command: execve(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: su

 Time:  1999-12-30 19:09:33.451448 EST
 UserName : bin  EffectiveName:   bin  AuditName: admin_u
 RUID: 2   EUID: 2   AUID: 2037   PID: 25352
 Command: execve(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: ls
```

Test 6: SUID program execs non-authored program (BSM_EXEC_NON_AUTHOR)

As user em_user1, run a program that is setuid to em_user2 and which exec:s a program owned by em_user1.

```
 Time:  1999-12-30 19:10:05.101532 EST
 UserName : em_user1  EffectiveName:   em_user2 AuditName:
em_user1
 RUID: 50001   EUID: 50002   AUID: 50001   PID: 25354
 Command: execve(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: sample
```

Test 7: Root Core File Created (BSM_ROOT_CORE_CREATE)

As root, run 'touch core' in a directory where there was no core file already.

```
 Time:  1999-12-30 19:10:40.051626 EST
 UserName : root  EffectiveName:   root  AuditName: admin_u
 RUID: 0   EUID: 0   AUID: 2037   PID: 25362
 Command: creat(2)   Ret_Val: 3   Error_Number: 0
 Parent Command: touch
 Path List: [ /export/home/core ]
 object_owner: (root|0)
```

Test 8: Root Core File Access (BSM_ROOT_CORE_ACCESS)

As em_user1, run 'file core' on a file called core owned by root, such as the one created for BSM_ROOT_CORE_CREATE.

```
 Time:  1999-12-30 19:11:09.361710 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25368
 Command: open(2) - read   Ret_Val: -1   Error_Number: 13
 Parent Command: file
 Path List: [ /export/home/core ]
 object_owner: (root|0)
```

Test 9: Change User Environment File (BSM_CHANGE_USER_ENVIRON_FILE)

As em_user1, use vi to create a new file .cshrc in a dir named em_user2.

```
 Time:  1999-12-30 19:12:56.712041 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25389
 Command: creat(2)   Ret_Val: 5   Error_Number: 0
 Parent Command: vi
 Path List: [ /usr/emerald/em_user2/.cshrc ]
```

Also as em_user1, run 'touch .rhosts' in a dir named em_user2 in which there was no .rhosts file already.

```
 Time:  1999-12-30 19:13:14.562088 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25391
 Command: creat(2)   Ret_Val: 3   Error_Number: 0
 Parent Command: touch
 Path List: [ /usr/emerald/em_user2/.rhosts ]
 object_owner: (em_user1|50001)

 Time:  1999-12-30 19:13:14.562088 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25391
 Command: old utime(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: touch
 Path List: [ /usr/emerald/em_user2/.rhosts ]
 object_owner: (em_user1|50001)
```

Test 10: Private File Access (BSM_ACCESS_PRIVATE_FILE)

As em_user2, run 'touch file1' where file1 is a file owned by em_user1 and whose full path begins with the prefix defined as location of home directories in BSM_USER_HOMES_LOCATION.

```
 Time:  1999-12-30 19:13:51.042193 EST
 UserName : em_user2  EffectiveName:   em_user2 AuditName:
em_user2
 RUID: 50002   EUID: 50002   AUID: 50002   PID: 25395
 Command: old utime(2)   Ret_Val: -1   Error_Number: 13
 Parent Command: touch
 Path List: [ /export/home/file1 ]
 object_owner: (em_user1|50001)
```

Test 11: Non-admin Enabled Setuid File (BSM_SUSPICIOUS_SETUID_ENABLER)

As em_user1, set the SUID bit on a file that you own, e g "chmod u+s gurka".

```
 Time:  1999-12-30 19:15:02.952379 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25402
 Command: chmod(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: chmod
 Path List: [ /usr/emerald/em_user1/gurka ]
 object_owner: (em_user1|50001)
```

Test 12: Non-owner Enabled Setuid File (BSM_SUSPICIOUS_SETUID_ATTACKER)

As em_user1, set the SUID bit on a file owned by em_user2. This is a little tricky, you need a program which is setuid to em_user2 that performs the chmod operation.

```
 Time:  1999-12-30 19:15:16.402415 EST
 UserName : em_user1  EffectiveName:   em_user2  AuditName:
em_user1
 RUID: 50001   EUID: 50002   AUID: 50001   PID: 25406
 Command: chmod(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: chmod
 Path List: [ /usr/emerald/em_user1/file_owned_by_2 ]
 object_owner: (em_user2|50002)
```

Test 13: Root core dump event (BSM_ROOT_CORE_EVENT)

As root, run for example 'sleep 20' and hit cntrl-\ (hold control and press backslash) while the program is running to force a core dump.

```
 Time:  1999-12-30 19:16:08.512544 EST
 UserName : root  EffectiveName:   root  AuditName: admin_u
 RUID: 0   EUID: 0   AUID: 2037   PID: 25411
 Command: process dumped core   Ret_Val: 0   Error_Number: 0
 Path List: [ /export/home/core ]
 object_owner: (root|0)
```

Test 14: Suspicious symlink creation (BSM_MAKE_TMP_SYM)

As em_user1, create a symbolic link in /tmp.

```
 Time:  1999-12-30 19:17:15.672732 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25420
 Command: symlink(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: ln
 Path List: [ /tmp/grepa ]
 object_owner: (em_user1|50001)
```

Test 15: Illegal (Shadow) Password Access Violation (BSM_ILLEGAL_SHADOW_PASSWD_ACCESS)

As em_user1, run 'rm /etc/shadow' (make sure you are NOT root!).

```
 Time:  1999-12-30 19:17:46.182810 EST
 UserName : em_user1  EffectiveName:   em_user1 AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25422
 Command: unlink(2)   Ret_Val: -1   Error_Number: 13
 Parent Command: rm
 Path List: [ /etc/shadow ]
 object_owner: (root|0)
```

Test 16: Promiscious Mode succeeded by non-admin user (BSM_PROMISCUOUS_MODE)

As em_user1, run a setuid root program which sets the network interface in promiscuous mode (e g tcpdump).

```
 Time:  1999-12-30 19:18:07.622872 EST
 UserName : em_user1  EffectiveName:   root  AuditName: em_user1
 RUID: 50001   EUID: 0   AUID: 50001   PID: 25424
 Command: open(2) - read,write   Ret_Val: 3   Error_Number: 0
 Parent Command: ./tcpdump
 Path List: [ /devices/pseudo/clone@0:hme ]
 object_owner: (root|0)
```

Test 17: Alteration to system executable BSM_MOD_SYSTEM_EXECUTABLE)

As root, make a modification to something in /usr/bin,
e g 'chmod g-x /usr/bin/who' and change it back again.

```
 Time:  1999-12-30 19:18:37.552959 EST
 UserName : root  EffectiveName:   root  AuditName: admin_u
 RUID: 0   EUID: 0   AUID: 2037   PID: 25426
 Command: chmod(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: chmod
 Path List: [ /usr/bin/who ]
 object_owner: (bin|2)

 Time:  1999-12-30 19:18:41.722972 EST
 UserName : root  EffectiveName:   root  AuditName: admin_u
 RUID: 0   EUID: 0   AUID: 2037   PID: 25427
 Command: chmod(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: chmod
 Path List: [ /usr/bin/who ]
 object_owner: (bin|2)
```

Test 18: Unpriv'd user changed system resource (BSM_MOD_SYSTEM_RESOURCE)

As em_user1, make a change to a directory in BSM_SYSTEM_LOG_LOCATIONS,
e g 'touch /var/log/.nasty'.

```
 Time:  1999-12-30 19:19:15.333061 EST
 UserName : em_user1  EffectiveName:   em_user1  AuditName:
em_user1
 RUID: 50001   EUID: 50001   AUID: 50001   PID: 25429
 Command: creat(2)   Ret_Val: -1   Error_Number: 13
 Parent Command: touch
 Path List: [ /var/log/.nasty ]
```

[Disabled loadmodule rules, now triggers BSM_SUSPICIOUS_SETUID_ENABLER twice]

Test 19: Root acquired by non-admin user (BSM_ROOT_BY_NONADMIN)

As em_user1, su to root.

```
 Time:  1999-12-30 19:21:36.283444 EST
 UserName : root  EffectiveName:   root  AuditName: em_user1
 RUID: 0   EUID: 0   AUID: 50001   PID: 25446
 Command: execve(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: tcsh
 Exec Args: [ tcsh ]
 Path List: [ /usr/bin/tcsh /usr/lib/ld.so.1 ]
 object_owner: (root|0)
```

Test 20: Admin SU performed by non-admin user (BSM_SETREUID_BY_NONADMIN)

As em_user1, su to em_admin.

[also triggered by the su to root test, if root is listed as an admin]

```
 Time:  1999-12-30 19:21:36.283444 EST
 UserName : root  EffectiveName:   root  AuditName: em_user1
 RUID: 0   EUID: 0   AUID: 50001   PID: 25446
 Command: old setuid(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: su
 Time:  1999-12-30 19:21:57.423508 EST
 UserName : em_admin  EffectiveName:   em_admin AuditName:
em_user1
 RUID: 50000   EUID: 50000   AUID: 50001   PID: 25448
 Command: old setuid(2)   Ret_Val: 0   Error_Number: 0
 Parent Command: su
```

Test 21: Maximum Bad Logins Reached (BSM_MAX_BAD_LOGINS)

Make repeated failed logins (mix invalid username/passwd).

```
 ([ invalid user name ]): login - telnet
 from (user invalid_username; UID 0) on host ?
 PID= 25456, time= 1999-12-30 19:25:40.634080 EST, sequence num-
ber= -1
 Etype = 6154, machineID = 130.107.15.118, error = 3

 ([ invalid password ]): login - telnet
 from (user em_user2; UID 50002) on host ?
 PID= 25456, time= 1999-12-30 19:25:30.734056 EST, sequence num-
ber= -1
 Etype= 6154, machineID= 130.107.15.118, error= 4

 ([ invalid password ]): login - telnet
 from (user em_user1; UID 50001) on host ?
 PID= 25456, time= 1999-12-30 19:25:11.564003 EST, sequence num-
ber= -1
 Etype= 6154, machineID= 130.107.15.118, error= 4

 ([ invalid password ]): login - telnet
 from (user em_user1; UID 50001) on host ?
 PID= 25456, time= 1999-12-30 19:25:04.483990 EST, sequence num-
ber= -1
 Etype= 6154, machineID= 130.107.15.118, error= 4
```

Test 22: Process exhaustion (BSM_PROC_EXHAUST_THRESHOLD)

Make fork() fail BSM_MAX_FAILED_PROCS_PER_CYCLE, times during BSM_FAILED_PROCS_THRESHOLD_WINDOW. This little C prog does the trick:

```
#include<signal.h>
#include <stdio.h>
#include <errno.h>
main()
{
  while( (fork()) >= 0  )
    ;
  perror("while1fork");
  sigsend(P_PGID, P_MYID, SIGKILL);
}
```

Be aware that this brings the machine to its knees for several minutes,
and can have some bizarre effects. Use with great caution!

```
 Start_time: 2000-01-05 20:45:34.375296 EST
 Command: fork(2)   Parent_cmd: not_present   Outcome: 11
     Attacker: em_user1
     Attacker_attrs: auid= 50001 ruid= 50001 euid= 50001 pid=
16307

                     sid= 15242
```

Test 23: File system exhaustion (BSM_FILE_EXHAUST_THRESHOLD)

Make a file system run out of inodes (preferably a floppy disk), and
then try to create a file there BSM_MAX_NOSPACE_ERRORS times within
BSM_WRITE_ERR_THRESHOLD_WINDOW.

This little C prog consumes all inodes:

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
main(int argc, char *argv[])
{
  int i, fd;
  char filename[FILENAME_MAX+1];
  if (argc != 2)
    {
      fprintf(stderr, "Usage: %s path\n", argv[0]);
      exit();
    }
  fprintf(stdout, "WARNING: This will consume all inodes on the

                       filesystem\n"
      "where %s is resided, by creating a very large number of empty \n"
      "files in %s. Hit Cntrl-C NOW if you do not want this to happen.\n"
      "Otherwise, hit the return key to proceed.\n", argv[1], argv[1]);
  getchar();
  fprintf(stdout, "Hold on while filling %s...\n", argv[1]);
  for( i= 0; 1; i++)
    {
       filename[0] = '\0';
       sprintf(filename, "%s/file%d", argv[1], i);
       fprintf(stderr, "Filename: %s\n", filename);
       if ( (fd = creat(filename, 0)) < 0 )
         {
            perror("creat()");
            exit();
         }
         close(fd);
   }
}
```

```
 Start_time: 2000-01-11 12:04:04.631142 EST
     Command: creat(2)   Parent_cmd: /usr/bin/tcsh   Outcome: 28

 Start_time: 2000-01-11 12:04:09.621150 EST
     Command: creat(2)   Parent_cmd: /usr/bin/tcsh   Outcome: 28
```

Test 24: Attempted root login on non-console terminal (BSM_ATTEMPTED_ROOT_LOGIN)

Try to telnet or rlogin as root.

```
  Start_time: 2000-01-11 12:51:56.836267 EST
 Command: login - telnet   Parent_cmd: <unknown-12782>   Outcome:
255

 Start_time: 2000-01-11 12:52:10.226282 EST
     Command: login - rlogin   Parent_cmd: <unknown-12785>   Out-
come: 255
```

Test 25: Port scanning (BSM_SUSPICIOUS_PORT_PROBE)

Run for example nmap against the host. Please note the following:

- Accept records are only produced on 5.6 and later
- Only TCP connect scans can produce accept records
- There must be a service responding on the port for an accept record to be produced

```
severity ports hit (port weight)  sum threshold

Warning  512(4), 21(3), 540(1), 13(1) 9 9
Severe warning 513(4), 21(3), 23(3), 25(3) 13 13
Attack  512(4), 21(3), 540(1), 13(1),
  513(4), 23(3), 7(1), 9(1) 18 18
```

```
    Start_time: 2000-01-14 11:12:34.378988 EST
    End_time: 2000-01-14 11:12:34.468992 EST
    Command: connect   Parent_cmd: not_present   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: target_ports = [ 13 540 512 21 ]

    Start_time: 2000-01-14 11:16:33.073903 EST
    End_time: 2000-01-14 11:16:33.993933 EST
    Command: connect   Parent_cmd: not_present   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: target_ports = [ 25 513 23 21 ]

    Start_time: 2000-01-14 11:21:49.210476 EST
    End_time: 2000-01-14 11:21:49.400490 EST
    Command: connect   Parent_cmd: not_present   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: target_ports = [ 13 9 7 540 512 513 23 21 ]
```

Test 26: External connection to forbidden port (BSM_BAD_PORT_CONN)

Telnet from a machine not listed in local_netmap.confn to one of the
ports in BSM_UNACCEPTABLE_PORT_CONNECTIONS, e g 514 (provided there is
a service responding on the victim port).

```
    Start_time: 2000-01-21 11:36:49.118565 EST
    Command: accept(2)   Parent_cmd: <unknown-137>   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: src_port = 1903  dst_port = 514
```

Test 27: FTP username guessing (BSM_FTP_UNAME_GUESSER)

Conect using FTP, and give invalid usernames BSM_MAX_FTP_BADPASSWORDS
within BSM_FAILED_LOGIN_WINDOW.

```
 ftp access,,Fri Jan 21 09:41:57 2000, + 82522111 msec,
 subject,-1,-1,-1,-1,-1,21110,21110,0 20 pooh.emerald.sri.com,
 text,unknown user APA,return,failure,2

 ftp access,,Fri Jan 21 09:42:03 2000, + 342394836 msec,
 subject,-1,-1,-1,-1,-1,21111,21111,0 20 pooh.emerald.sri.com,
 text,unknown user bepa,return,failure,2

 ftp access,,Fri Jan 21 09:42:16 2000, + 292135865 msec,
 subject,-1,-1,-1,-1,-1,21112,21112,0 20 pooh.emerald.sri.com,
 text,unknown user cepa,return,failure,2

 ftp access,,Fri Jan 21 09:42:20 2000, + 752048324 msec,
 subject,-1,-1,-1,-1,-1,21113,21113,0 20 pooh.emerald.sri.com,
 text,unknown user depa,return,failure,2

 ftp access,,Fri Jan 21 09:42:30 2000, + 71863177 msec,
 subject,-1,-1,-1,-1,-1,21114,21114,0 20 pooh.emerald.sri.com,
 text,unknown user fepa,return,failure,2
 ftp access,,Fri Jan 21 09:42:36 2000, + 31742396 msec,
 subject,-1,-1,-1,-1,-1,21115,21115,0 20 pooh.emerald.sri.com,
 text,unknown user gepa,return,failure,2

 ftp access,,Fri Jan 21 09:42:44 2000, + 21586038 msec,
 subject,-1,-1,-1,-1,-1,21116,21116,0 20 pooh.emerald.sri.com,
 text,unknown user hepa,return,failure,2
```

Test 28: FTP password guessing (BSM_FTP_PASSWD_GUESSER)

Conect using FTP, and give valid usernames but invalid passwords BSM_MAX_FTP_BADPASSWORDS within BSM_FAILED_LOGIN_WINDOW.

```
 ftp access,,Fri Jan 21 09:47:23 2000, + 46354724 msec,
 subject,50001,50001,512,50001,512,21127,21127,0 20
 pooh.emerald.sri.com,text,bad password,return,failure,1

 ftp access,,Fri Jan 21 09:47:36 2000, + 236091094 msec,
 subject,50002,50002,512,50002,512,21128,21128,0 20
 pooh.emerald.sri.com,text,bad password,return,failure,1

 ftp access,,Fri Jan 21 09:47:45 2000, + 455911912 msec,
        subject,50001,50001,512,50001,512,21129,21129,0 20
 pooh.emerald.sri.com,text,bad password,return,failure,1

 ftp access,,Fri Jan 21 09:47:56 2000, + 715689103 msec,
 subject,50000,50000,512,50000,512,21130,21130,0 20
 pooh.emerald.sri.com,text,bad password,return,failure,1

 ftp access,,Fri Jan 21 09:48:06 2000, + 925481601 msec,
 subject,50001,50001,512,50001,512,21131,21131,0 20
 pooh.emerald.sri.com,text,bad password,return,failure,1

 ftp access,,Fri Jan 21 09:48:16 2000, + 945280661 msec,
 subject,50001,50001,512,50001,512,21132,21132,0 20
 pooh.emerald.sri.com,text,bad password,return,failure,1
```

Test 28: FTP anonymous write (BSM_FTP_ANON_WRITE)

FTP in as user 'ftp' or 'anonymous' and upload a file to a directory which is not in BSM_FTP_UPLOAD_PATHS.

```
 open(2) - write,creat,trunc,,Fri Jan 21 09:52:09 2000,
 + 850943250 msec,path,/usr/local/ftp/pub/upload/passwd,
 attribute,100666,65533,65533,8388614,80160,0,
 subject,-2,65533,65533,root,root,21147,0,0 0 0.0.0.0,
 return,success,4

 chown(2),,Fri Jan 21 09:52:09 2000, + 870945353 msec,
 argument,2,0xfffd,new file uid,argument,3,0xffffffff,
 new file gid,path,/usr/local/ftp/pub/upload/passwd,
 attribute,100666,65533,65533,8388614,80160,0,
 subject,-2,65533,65533,root,root,21147,0,0 0 0.0.0.0,
 return,success,0

 open(2) - write,creat,trunc,,Fri Jan 21 09:54:08 2000,
 + 168689095 msec,path,/usr/local/ftp/pub/warez/win2000,
 attribute,100666,65533,65533,8388614,137088,0,
 subject,-2,65533,65533,root,root,21154,0,0 0 0.0.0.0,
 return,success,4

 chown(2),,Fri Jan 21 09:54:08 2000, + 188688803 msec,
 argument,2,0xfffd,new file uid,argument,3,0xffffffff,
 new file gid,path,/usr/local/ftp/pub/warez/win2000,
 attribute,100666,65533,65533,8388614,137088,0,
 subject,-2,65533,65533,root,root,21154,0,0 0 0.0.0.0,
 return,success,0
```

Test 29: FTP 'warez' activity (BSM_FTP_WAREZ_ACTIVITY)

Upload a file anonymously and then download it in BSM_FTP_WAREZ_COMPLAINT anonymous sessions.

```
open(2) - read,,Fri Jan 21 09:54:25 2000, + 938331667 msec,
path,/usr/local/ftp/pub/warez/win2000,
attribute,100666,65533,65533,8388614,137088,0,
subject,-2,65533,65533,root,root,21156,0,0 0 0.0.0.0,
return,success,4

Repeated on the following times:

Fri Jan 21 09:55:03 2000, + 937574993 msec
Fri Jan 21 09:55:23 2000, + 417191074 msec
Fri Jan 21 09:55:42 2000, + 416812353 msec
Fri Jan 21 09:55:57 2000, + 506512892 msec
Fri Jan 21 09:56:13 2000, + 416197895 msec
Fri Jan 21 09:56:27 2000, + 25943165 msec
Fri Jan 21 09:56:42 2000, + 95650128 msec
```

Test 30: Inetd exhaustion (BSM_CLIENT_INET_WATCH)

```
telnet victim >& /dev/null & telnet victim >& /dev/null &
```

etc for at least BSM_MAX_CLIENT_PROCS_PER_CYCLE connects in total during BSM_EXTERNAL_CONN_THRESHOLD_WINDOW.

NOTE: sisko (5.6) did not produce inetd records, but owl (5.5.1) did.

```
 inetd,,Mon Feb 07 19:29:20 2000, + 916180946 msec,
 subject,root,root,root,root,root,0,0,0 0
sevenof9.emerald.sri.com,
 text,telnet,ip address,sevenof9.emerald.sri.com,ip port,0x8043,
 return,success,0

 Repeated on the following times:

 Mon Feb 07 19:29:20 2000, + 966180837
 Mon Feb 07 19:29:21 2000, + 46180242
 Mon Feb 07 19:29:21 2000, + 126183000
 Mon Feb 07 19:29:21 2000, + 196182216
 Mon Feb 07 19:29:21 2000, + 266183540
 Mon Feb 07 19:29:21 2000, + 326185824
 Mon Feb 07 19:29:21 2000, + 396185327
```

Test 31: Access policy for direct access

```
as  run   result   policy

em_user1 /usr/sbin/iffconfig failure  disallowed
em_user1 /usr/sbin/ifconfig success  disallowed
em_user1 cat /secret/file  failure  disallowed
em_user1 cat /accounting/DBMS/payroll.db success disallowed
em_accnt cat /accounting/DBMS/payroll.db success allowed
em_user1 rm /accounting/DBMS/payroll.db failure  disallowed
(a chmod in between)
em_user1 rm /accounting/DBMS/payroll.db success  disallowed
```

Test 32: Access policy with respect to ftp

```
FTP in as       run                 result  policy

em_user1  get /secret/file file                 failure disallowed
em_user1  get /accounting/DBMS/payroll.db payroll.db  success disallowed

em_admin  get /secret/file file                       failure allowed
em_admin  get /accounting/DBMS/payroll.db payroll.db  success allowed

ftp   put ls /bin/ls                failure disallowed
                 (translates to /usr/local/ftp/usr/bin/ls)
```

Test 33: Time warp (BSM_TIMEWARP)

To the end of the stream of audit records, add a single record which
has a timestamp that is at least BSM_MAX_BACKWARD_TIME earlier

than
the previously last record, for example

```
cat singlerec.bsm >> big_test.bsm
```

where singlerec.bsm contains a single accept record with timestamp
Fri Jan 21 08:11:13 2000, + 118566453 msec

Appendix II: Attack Battery Console Alerts

```
PBEST runtime library built  Wed Oct 6 09:56:34 PDT 1999
User Map [/usr/emerald/test/final/Emerald_eXpert_BSM_v1.4/resource-object/config-
TEST/username_map.conf] Loaded Successfully

-------------------------------------------------------------
EMERALD eXpert P-BEST Signature Engine
An unpublished work of SRI International
System Design Laboratory, SRI International
All Rights Reserved. EMERALD (tm) Trademark SRI International.

Direct all comments or questions to: emerald-release@sdl.sri.com

Monitor Started: Sat Sep 29 17:28:21 2001

Operating from:
    Hostname: kess
    IP Address: 130.107.12.70
    Report Log: <STDOUT>
-------------------------------------------------------------

Loading Internal IP List (/usr/emerald/test/final/Emerald_eXpert_BSM_v1.4/resource-
object/config//local_netmap.conf)...load complete.
Access Policy Configuration File [/usr/emerald/test/final/Emerald_eXpert_BSM_v1.4/resource-
object/config//accesspolicy.conf] Loaded Successfully

--------------------------------------------------------------
ATTACK  (1|1|2)  BSM_BUFFER_OVERFLOW_EXEC   Target: 197.218.177.69   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1998-07-29 16:27:29.562456 PDT
    Command: execve(2)   Parent_cmd: /usr/bin/ps   Outcome: 0
    Attacker: user_v
    Attacker_attrs: auid = 2053  ruid = 2053  euid = 0  pid = 5593  sid = 5584
    Command_arg: ps
    Resource: /usr/bin/ps   Resource_owner: root
    Recommendation: lockout -uname user_v -da kess; killall -uname user_v -pid 5593 -da kess
    Comment: root compromise

--------------------------------------------------------------
SEVERE WARNING  (2|2|6309)  BSM_SELF_ECHO_ALERT   Target: 130.107.12.70   Count: 6306
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-04-05 17:17:10.001999 PDT   End_time: 1999-04-05 17:18:09.992008 PDT
    Command: echo   Parent_cmd: inetd   Outcome: 0
    Attacker: 172.16.114.50
    Recommendation: checkcfg -da kess -name BSM_MAX_ECHOS_RECEIVED; checkcfg -da kess
    -name BSM_ECHO_FLOOD_WINDOW
    Comment: relevant params: BSM_MAX_ECHOS_RECEIVED, BSM_ECHO_FLOOD_WINDOW

--------------------------------------------------------------
ATTACK  (3|3|6562)  BSM_BUFFER_OVERFLOW_EXEC   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:08:13.371242 PST
    Command: execve(2)   Parent_cmd: /usr/bin/eject   Outcome: 0
    Attacker: admin_u
    Attacker_attrs: auid = 2037  ruid = 2037  euid = 0  pid = 25345  sid = 24792
    Command_arg: eject
    Resource: /usr/bin/eject   Resource_owner: root
    Recommendation: lockout -uname admin_u -da kess; killall -uname admin_u -pid 25345
    -da kess
    Comment: root compromise

---------------------------------------------------------------
WARNING  (4|4|6575)  BSM_SUSPICIOUS_EXEC_ARGUMENT   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:08:51.011335 PST
    Command: execve(2)   Parent_cmd: /usr/bin/anyexploitany   Outcome: 2
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 25346  sid = 25336
    Resource: /usr/bin/anyexploitany   Resource_owner: not_present
    Recommendation: fixperms -fn /usr/bin/anyexploitany -da kess -newattr 000; checkcfg
    -da kess -name BSM_SUSPICIOUS_EXEC_LIST
    Comment: relevant params: BSM_SUSPICIOUS_EXEC_LIST

---------------------------------------------------------------
WARNING  (5|5|6576)  BSM_SUSPICIOUS_EXEC_ARGUMENT   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:08:51.011335 PST
    Command: execve(2)   Parent_cmd: /usr/emerald/em_user1/anyexploitany   Outcome: 2
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 25346  sid = 25336
    Resource: /usr/emerald/em_user1/anyexploitany   Resource_owner: not_present
    Recommendation: fixperms -fn /usr/emerald/em_user1/anyexploitany -da kess
    -newattr 000; checkcfg -da kess -name BSM_SUSPICIOUS_EXEC_LIST
    Comment: relevant params: BSM_SUSPICIOUS_EXEC_LIST

---------------------------------------------------------------
ATTACK  (6|6|6644)  BSM_SPECIAL_USER_EXEC   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:09:27.631431 PST
    Command: execve(2)   Parent_cmd: /usr/bin/sh   Outcome: 0
    Attacker: bin
    Attacker_attrs: auid = 2037  ruid = 2  euid = 2  pid = 25350  sid = 25039
    Command_arg: su
    Resource: /usr/bin/sh   Resource_owner: bin
    Recommendation: killall -uname admin_u -pid 25350 -da kess; checkcfg -da kess
    -name BSM_EXEC_LESS_ACCOUNTS
    Comment: relevant params: BSM_EXEC_LESS_ACCOUNTS

---------------------------------------------------------------
ATTACK  (7|7|6652)  BSM_SPECIAL_USER_EXEC   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:09:33.451448 PST
    Command: execve(2)   Parent_cmd: /usr/bin/ls   Outcome: 0
    Attacker: bin
    Attacker_attrs: auid = 2037  ruid = 2  euid = 2  pid = 25352  sid = 25039
    Command_arg: ls
    Resource: /usr/bin/ls   Resource_owner: bin
    Recommendation: killall -uname admin_u -pid 25352 -da kess; checkcfg -da kess
    -name BSM_EXEC_LESS_ACCOUNTS
    Comment: relevant params: BSM_EXEC_LESS_ACCOUNTS

---------------------------------------------------------------
ATTACK  (8|8|6676)  BSM_EXEC_NON_AUTHOR   Target: 130.107.15.118   Count: 1
```

```
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:10:05.101532 PST
    Command: execve(2)   Parent_cmd: /usr/emerald/em_user1/sample   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50002  pid = 25354  sid = 25336
    Command_arg: sample
    Resource: /usr/emerald/em_user1/sample   Resource_owner: em_user1
    Recommendation: killall -uname em_user1 -pid 25354 -da kess; fixperms -fn
    /usr/emerald/em_user1/sample -da kess -newattr 000; notify -uid 50001 -da kess;
    checkcfg -da kess -name BSM_LAST_RESERVED_ACCOUNT
    Comment: relevant params: BSM_LAST_RESERVED_ACCOUNT

---------------------------------------------------------------
WARNING  (9|9|6743)  BSM_ROOT_CORE_CREATE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:10:40.051626 PST
    Command: creat(2)   Parent_cmd: /usr/bin/touch   Outcome: 0
    Attacker: admin_u
    Attacker_attrs: auid = 2037  ruid = 0  euid = 0  pid = 25362  sid = 25039
    Resource: /export/home/core   Resource_owner: root
    Recommendation: fixperms -fn /export/home/core -da kess -newattr 000

---------------------------------------------------------------
SEVERE WARNING  (10|10|6834)  BSM_ROOT_CORE_ACCESS   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:11:09.361710 PST
    Command: open(2) - read   Parent_cmd: /usr/bin/file   Outcome: 13
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 25368  sid = 25336
    Resource: /export/home/core   Resource_owner: root
    Recommendation: kill -pid 25368 -sid 25336 -da kess; fixperms -fn /export/home/core
    -da kess -newattr 000

---------------------------------------------------------------
ATTACK  (11|11|7231)  BSM_CHANGE_USER_ENVIRON_FILE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:13:26.812124 PST
    Command: unlink(2)   Parent_cmd: /usr/bin/rm   Outcome: 0
    Attacker: em_user2
    Attacker_attrs: auid = 50002  ruid = 50002  euid = 50002  pid = 25393  sid = 25372
    Resource: /usr/emerald/em_user2/.rhosts   Resource_owner: em_user1
    Recommendation: fixperms -fn /usr/emerald/em_user2/.rhosts -da kess -newattr 000;
    fixperms -fn /usr/emerald/em_user2/.rhosts -da kess –newname
    /usr/emerald/em_user2/.rhosts.corrupted-by-em_user2; notify -uid 50001 -da kess;
    checkcfg -da kess -name BSM_USER_ENV_FILES
    Comment: relevant params: BSM_USER_ENV_FILES

---------------------------------------------------------------
SEVERE WARNING  (12|12|7254)  BSM_ACCESS_PRIVATE_FILE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:13:51.042193 PST
    Command: old utime(2)   Parent_cmd: /usr/bin/touch   Outcome: 13
    Attacker: em_user2
    Attacker_attrs: auid = 50002  ruid = 50002  euid = 50002  pid = 25395  sid = 25372
    Resource: /export/home/file1   Resource_owner: em_user1
    Recommendation: fixperms -fn /export/home/file1 -da kess -newattr 000; notify -uid
    50001 -da kess; checkcfg -da kess -name BSM_USER_HOMES_LOCATIONS
    Comment: relevant params: BSM_USER_HOMES_LOCATION
```

```
--------------------------------------------------------------
WARNING  (13|13|7323)  BSM_SUSPICIOUS_SETUID   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:15:02.952379 PST
    Command: chmod(2)   Parent_cmd: /usr/bin/chmod   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 25402  sid = 25336
    Resource: /usr/emerald/em_user1/gurka   Resource_owner: em_user1
    Recommendation: fixperms -fn /usr/emerald/em_user1/gurka -da kess -newattr 000; kill
    -pid 25402 -sid 25336 -da kess; notify -uid 50001 -da kess; checkcfg -da kess -name
    BSM_ADMINISTRATIVE_USER_LIST
    Comment: relevant-params: BSM_ADMINISTRATIVE_USER_LIST

--------------------------------------------------------------
ATTACK  (14|14|7355)  BSM_SUSPICIOUS_SETUID   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:15:16.402415 PST
    Command: chmod(2)   Parent_cmd: /usr/bin/chmod   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50002  pid = 25406  sid = 25336
    Resource: /usr/emerald/em_user1/file_owned_by_2   Resource_owner: em_user2
    Recommendation: fixperms -fn /usr/emerald/em_user1/file_owned_by_2 -da kess –newattr
    000; kill -pid 25406 -sid 25336 -da kess; notify -uid 50002 -da kess; checkcfg -da kess
    -name BSM_ADMINISTRATIVE_USER_LIST
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST

--------------------------------------------------------------
SEVERE WARNING  (15|15|7401)  BSM_ROOT_CORE_EVENT   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:16:08.512544 PST
    Command: coredump   Parent_cmd: not_present   Outcome: 0
    Attacker: admin_u
    Attacker_attrs: auid = 2037  ruid = 0  euid = 0  pid = 25411  sid = 25039
    Resource: /export/home/core   Resource_owner: root
    Recommendation: fixperms -fn /export/home/core -da kess -newattr 000

--------------------------------------------------------------
ATTACK  (16|16|7528)  BSM_ILLEGAL_SHADOW_PASSWD_ACCESS   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:17:46.182810 PST
    Command: unlink(2)   Parent_cmd: /usr/bin/rm   Outcome: 13
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 25422  sid = 25336
    Resource: /etc/shadow   Resource_owner: root
    Recommendation: killall -uname em_user1 -pid 25422 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name BSM_ADMINISTRATIVE_USER_LIST
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST

--------------------------------------------------------------
ATTACK  (17|17|7553)  BSM_PROMISCUOUS_MODE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:18:07.622872 PST
    Command: open(2) - read,write   Parent_cmd: /usr/emerald/em_user1/tcpdump   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 0  pid = 25424  sid = 25336
    Resource: /devices/pseudo/clone@0:hme   Resource_owner: root
    Recommendation: killall -uname em_user1 -pid 25424 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name BSM_ADMINISTRATIVE_USER_LIST; checkcfg -da kess
   -name BSM_EMERALD_NIC_NAMES
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST, BSM_EMERALD_NIC_NAMES

--------------------------------------------------------------
```

```
WARNING  (18|18|7591)  BSM_MOD_SYSTEM_EXECUTABLE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:18:37.552959 PST
    Command: chmod(2)   Parent_cmd: /usr/bin/chmod   Outcome: 0
    Attacker: admin_u
    Attacker_attrs: auid = 2037  ruid = 0  euid = 0  pid = 25426  sid = 25039
    Resource: /usr/bin/who   Resource_owner: bin
    Recommendation: killall -uname admin_u -pid 25426 -da kess; lockout -uname admin_u
    -da kess; fixperms -fn /usr/bin/who -da kess -newattr 000; checkcfg -da kess -name
    BSM_SYSTEM_BIN_LOCATIONS
    Comment: relevant params: BSM_SYSTEM_BIN_LOCATIONS

--------------------------------------------------------------
WARNING  (19|19|7600)  BSM_MOD_SYSTEM_EXECUTABLE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:18:41.722972 PST
    Command: chmod(2)   Parent_cmd: /usr/bin/chmod   Outcome: 0
    Attacker: admin_u
    Attacker_attrs: auid = 2037  ruid = 0  euid = 0  pid = 25427  sid = 25039
    Resource: /usr/bin/who   Resource_owner: bin
    Recommendation: killall -uname admin_u -pid 25427 -da kess; lockout -uname admin_u
    -da kess; fixperms -fn /usr/bin/who -da kess -newattr 000; checkcfg -da kess -name
    BSM_SYSTEM_BIN_LOCATIONS
    Comment: relevant params: BSM_SYSTEM_BIN_LOCATIONS

--------------------------------------------------------------
SEVERE WARNING  (20|20|7620)  BSM_MOD_SYSTEM_RESOURCE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:19:15.333061 PST
    Command: creat(2)   Parent_cmd: /usr/bin/touch   Outcome: 13
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 25429  sid = 25336
    Resource: /var/log/.nasty   Resource_owner: not_present
    Recommendation: killall -uname em_user1 -pid 25429 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name BSM_SYSTEM_LOG_LOCATIONS; checkcfg -da kess -name
    BSM_SYSTEM_RESOURCE_FILES; checkcfg -da kess -name BSM_SYSTEM_RESERVED_ACCOUNTS
    Comment: relevant params: BSM_SYSTEM_LOG_LOCATIONS BSM_SYSTEM_RESOURCE_FILES
    BSM_LAST_RESERVED_ACCOUNT

--------------------------------------------------------------
WARNING  (21|21|7695)  BSM_SUSPICIOUS_SETUID   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:20:01.183188 PST
    Command: chmod(2)   Parent_cmd: /usr/bin/chmod   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 25436  sid = 25336
    Resource: /usr/emerald/em_user1/csh   Resource_owner: em_user1
    Recommendation: fixperms -fn /usr/emerald/em_user1/csh -da kess -newattr 000; kill
    -pid 25436 -sid 25336 -da kess; notify -uid 50001 -da kess; checkcfg -da kess -name
    BSM_ADMINISTRATIVE_USER_LIST
    Comment: relevant-params: BSM_ADMINISTRATIVE_USER_LIST

--------------------------------------------------------------
WARNING  (22|22|7775)  BSM_SUSPICIOUS_SETUID   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:20:48.143320 PST
    Command: chmod(2)   Parent_cmd: /usr/bin/chmod   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 25443  sid = 25336
    Resource: /tmp/gurka   Resource_owner: em_user1
    Recommendation: fixperms -fn /tmp/gurka -da kess -newattr 000; kill -pid 25443
    -sid 25336 -da kess; notify -uid 50001 -da kess; checkcfg -da kess -name
    BSM_ADMINISTRATIVE_USER_LIST
    Comment: relevant-params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
ATTACK  (23|23|7864)  BSM_ROOT_BY_NONADMIN   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:21:36.283444 PST
    Command: old setuid(2)   Parent_cmd: /usr/bin/su   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 0  euid = 0  pid = 25446  sid = 25336
    Recommendation: kill -pid 25446 -sid 25336 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name BSM_ADMINISTRATIVE_USER_LIST; checkcfg -da kess
    -name BSM_NONADMIN_EXPIRE
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST BSM_NONADMIN_EXPIRE

---------------------------------------------------------------
ATTACK  (24|24|7970)  BSM_ROOT_BY_NONADMIN   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:21:57.423508 PST
    Command: old setuid(2)   Parent_cmd: /usr/bin/su   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50000  euid = 50000  pid = 25448  sid = 25336
    Recommendation: kill -pid 25448 -sid 25336 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name BSM_ADMINISTRATIVE_USER_LIST; checkcfg -da kess -name
    BSM_NONADMIN_EXPIRE
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST BSM_NONADMIN_EXPIRE

---------------------------------------------------------------
ATTACK  (25|25|8071)  BSM_ROOT_BY_NONADMIN   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:22:23.663584 PST
    Command: old setuid(2)   Parent_cmd: /usr/bin/su   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50002  euid = 50002  pid = 25451  sid = 25336
    Recommendation: kill -pid 25451 -sid 25336 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name BSM_ADMINISTRATIVE_USER_LIST; checkcfg -da kess
    -name BSM_NONADMIN_EXPIRE
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST BSM_NONADMIN_EXPIRE

---------------------------------------------------------------
WARNING  (26|26|8230)  BSM_REACH_MAX_BADLOGIN   Target: kess   Count: 4
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:25:40.634080 PST
    Command: login - telnet   Parent_cmd: /usr/bin/login   Outcome: -1
    Attacker: not_present
    Recommendation: filter -sa ? -da kess; checkcfg -da kess -name BSM_MAX_LOGIN_THRESHOLD;
    checkcfg -da kess -name BSM_FAILED_LOGIN_WINDOW
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST BSM_NONADMIN_EXPIRE
    Comment: 130.107.15.118 login - telnet [ invalid user name ] from invalid username
    Comment: 130.107.15.118 login - telnet [ invalid password ] from em_user2
    Comment: 130.107.15.118 login - telnet [ invalid password ] from em_user1
    Comment: 130.107.15.118 login - telnet [ invalid password ] from em_user1
    Comment: relevant params: BSM_MAX_LOGIN_THRESHOLD, BSM_FAILED_LOGIN_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (27|27|8569)  BSM_PROC_EXHAUST_THRESHOLD   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-05 17:45:34.375296 PST
    Command: fork(2)   Parent_cmd: not_present   Outcome: 11
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 16307  sid = 15242
    Recommendation: checkcfg -da kess -name BSM_MAX_FAILED_PROCS_PER_CYCLE; checkcfg
    -da kess -name BSM_FAILED_PROCS_THRESHOLD_WINDOW
    Comment: relevant params: BSM_MAX_FAILED_PROCS_PER_CYCLE,
    BSM_FAILED_PROCS_THRESHOLD_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (28|28|8723)  BSM_FILE_EXHAUST_THRESHOLD   Target: 130.107.15.118   Count: 8
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-11 09:04:04.631142 PST
    Command: creat(2)   Parent_cmd: /usr/bin/tcsh   Outcome: 28
    Attacker: non_present
    Recommendation: diagnose -fs /mnt/floppy/sample3 -da kess; checkcfg -da kess -name
    BSM_MAX_NOSPACE_ERRORS; checkcfg -da kess -name BSM_WRITE_ERR_THRESHOLD_WINDOW
    Comment: relevant params: BSM_MAX_NOSPACE_ERRORS, BSM_WRITE_ERR_THRESHOLD_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (29|29|8731)  BSM_FILE_EXHAUST_THRESHOLD   Target: 130.107.15.118   Count: 8
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-11 09:04:09.621150 PST
    Command: creat(2)   Parent_cmd: /usr/bin/tcsh   Outcome: 28
    Attacker: non_present
    Recommendation: diagnose -fs /mnt/floppy/sample3 -da kess; checkcfg -da kess
    -name BSM_MAX_NOSPACE_ERRORS; checkcfg -da kess -name BSM_WRITE_ERR_THRESHOLD_WINDOW
    Comment: relevant params: BSM_MAX_NOSPACE_ERRORS, BSM_WRITE_ERR_THRESHOLD_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (30|30|8766)  BSM_ATTEMPTED_ROOT_LOGIN   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-11 09:51:56.836267 PST
    Command: login - telnet   Parent_cmd: <unknown-12782>   Outcome: 255
    Attacker: 130.107.15.118
    Attacker_attrs: auid = 0  ruid = 0  euid = 0  pid = 12782  sid = 12782
    Recommendation: filter -sa 130.107.15.118 -da kess
    Comment: Attempted remote root login

---------------------------------------------------------------
SEVERE WARNING  (31|31|8768)  BSM_ATTEMPTED_ROOT_LOGIN   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-11 09:52:10.226282 PST
    Command: login - rlogin   Parent_cmd: <unknown-12785>   Outcome: 255
    Attacker: 130.107.15.118
    Attacker_attrs: auid = 0  ruid = 0  euid = 0  pid = 12785  sid = 12785
    Recommendation: filter -sa 130.107.15.118 -da kess
    Comment: Attempted remote root login

---------------------------------------------------------------
WARNING  (32|32|9530)  BSM_SUSPICIOUS_PORT_PROBE   Target: 130.107.12.70   Count: 4
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-14 08:12:34.378988 PST   End_time: 2000-01-14 08:12:34.468992 PST
    Command: connect   Parent_cmd: not_present   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: target_ports = [ 13 540 512 21 ]
    Recommendation: filter -sa 130.107.15.118 -da kess; checkcfg -da kess -name
    BSM_PORTHIT_WARNING; checkcfg -da kess -name BSM_PORT_ANALYSIS_WINDOW
    Comment: relevant params: BSM_PORTHIT_WARNING, BSM_PORT_ANALYSIS_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (33|33|9677)  BSM_SUSPICIOUS_PORT_PROBE   Target: 130.107.12.70   Count: 4
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-14 08:16:33.073903 PST   End_time: 2000-01-14 08:16:33.993933 PST
    Command: connect   Parent_cmd: not_present   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: target_ports = [ 25 513 23 21 ]
    Recommendation: filter -sa 130.107.15.118 -da kess; checkcfg -da kess -name
    BSM_PORTHIT_WARNING; checkcfg -da kess -name BSM_PORT_ANALYSIS_WINDOW
    Comment: relevant params: BSM_PORTHIT_WARNING, BSM_PORT_ANALYSIS_WINDOW

---------------------------------------------------------------
ATTACK  (34|34|9890)  BSM_SUSPICIOUS_PORT_PROBE   Target: 130.107.12.70   Count: 8
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-14 08:21:49.210476 PST   End_time: 2000-01-14 08:21:49.400490 PST
    Command: connect   Parent_cmd: not_present   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: target_ports = [ 13 9 7 540 512 513 23 21 ]
    Recommendation: filter -sa 130.107.15.118 -da kess; checkcfg -da kess -name
    BSM_PORTHIT_WARNING; checkcfg -da kess -name BSM_PORT_ANALYSIS_WINDOW
    Comment: relevant params: BSM_PORTHIT_WARNING, BSM_PORT_ANALYSIS_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (35|35|10065)  BSM_BAD_PORT_CONNECTION   Target: kess   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 08:36:49.118565 PST
    Command: accept(2)   Parent_cmd: <unknown-137>   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: src_port = 1903  dst_port = 514
    Recommendation: filter -sa 130.107.15.118 -da kess; checkcfg -da kess -name
    BSM_MAX_CONN_FACTS; checkcfg -da kess -name BSM_PORT_ANALYSIS_WINDOW
    Comment: relevant params: BSM_UNACCEPTABLE_PORT_CONNECTIONS, host and net lists in
/usr/emerald/test/final/Emerald_eXpert_BSM_v1.4/resource-object/config//local_netmap.conf

---------------------------------------------------------------
SEVERE WARNING  (36|36|10222)  BSM_FTP_USERNAME_GUESSER   Target: kess   Count: 5
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 09:41:57.082521 PST   End_time: 2000-01-21 09:42:30.071862 PST
    Command: open(2) - read,write   Parent_cmd: <unknown-122>   Outcome: 0
    Attacker: 130.107.12.103
    Attacker_attrs: auid = 0  ruid = 0  euid = 0  pid = 122  sid = 0
    Recommendation: filter -sa 130.107.12.103 -da kess -dp 21; checkcfg -da kess
    -name BSM_MAX_FTP_BADPASSWORDS; checkcfg -da kess -name BSM_FAILED_LOGIN_WINDOW
    Comment: relevant params: BSM_MAX_FTP_BADPASSWORDS, BSM_FAILED_LOGIN_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (37|37|10444)  BSM_FTP_PASSWD_GUESSER   Target: kess   Count: 4
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 09:47:23.046354 PST   End_time: 2000-01-21 09:48:00.235610 PST
    Command: open(2) - read,write   Parent_cmd: <unknown-122>   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: src_ip = 130.107.12.103  auid = 0  ruid = 0  euid = 0  pid = 122 sid = 0
    Recommendation: filter -sa 130.107.12.103 -da kess -dp 21; checkcfg -da kess -name
    BSM_MAX_FTP_BADPASSWORDS; checkcfg -da kess -name BSM_FAILED_LOGIN_WINDOW
    Comment: relevant params: BSM_MAX_FTP_BADPASSWORDS BSM_FAILED_LOGIN_WINDOW

---------------------------------------------------------------
ATTACK  (38|38|10599)  BSM_FTP_ANON_WRITE   Target: kess   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 09:52:09.850942 PST
    Command: open(2) - write,creat,trunc   Parent_cmd: /usr/sbin/in.ftpd   Outcome: 0
    Attacker: 130.107.12.103
    Attacker_attrs: auid = 0  ruid = 0  euid = 65533  pid = 21147  sid = 0
    Resource: /usr/local/ftp/pub/upload/passwd   Resource_owner: ftp
    Recommendation: reset -sa 130.107.12.103 -da kess -dp 21; kill -pid 21147 -sid 0 -da
    kess; checkcfg -da kess -name BSM_ANON_FILE_EXPIRE; checkcfg -da kess -name
    BSM_LOCAL_FTPD_UID; checkcfg -da kess -name BSM_ANON_FTP_MONITOR_WINDOW; checkcfg
   -da kess -name BSM_FTP_UPLOAD_PATHS
    Comment: relevant params: BSM_ANON_FILE_EXPIRE BSM_LOCAL_FTPD_UID
```

```
BSM_ANON_FTP_MONITOR_WINDOW BSM_FTP_UPLOAD_PATHS

---------------------------------------------------------------
ATTACK  (39|39|10693)  BSM_FTP_ANON_WRITE   Target: kess   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 09:54:08.168688 PST
    Command: open(2) - write,creat,trunc   Parent_cmd: /usr/sbin/in.ftpd   Outcome: 0
    Attacker: 130.107.12.103
    Attacker_attrs: auid = 0  ruid = 0  euid = 65533  pid = 21154  sid = 0
    Resource: /usr/local/ftp/pub/warez/win2000   Resource_owner: ftp
    Recommendation: reset -sa 130.107.12.103 -da kess -dp 21; kill -pid 21154 -sid 0
    -da kess; checkcfg -da kess -name BSM_ANON_FILE_EXPIRE; checkcfg -da kess -name
    BSM_LOCAL_FTPD_UID; checkcfg -da kess -name BSM_ANON_FTP_MONITOR_WINDOW; checkcfg
    -da kess -name BSM_FTP_UPLOAD_PATHS
    Comment: relevant params: BSM_ANON_FILE_EXPIRE BSM_LOCAL_FTPD_UID
    BSM_ANON_FTP_MONITOR_WINDOW BSM_FTP_UPLOAD_PATHS

---------------------------------------------------------------
WARNING  (40|40|10949)  BSM_FTP_WAREZ_ACTIVITY   Target: not_present   Count: 5
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 09:54:08.188687 PST   End_time: 2000-01-21 09:55:57.506511 PST
    Command: open(2) - read   Parent_cmd: /usr/sbin/in.ftpd   Outcome: 0
    Attacker: root
    Attacker_attrs: auid = 0  ruid = 0  euid = 65533  pid = 21160  sid = 0
    Resource: /usr/local/ftp/pub/warez/win2000   Resource_owner: ftp
    Recommendation: fixperms -fn [ /usr/local/ftp/pub/warez/win2000 ] -da kess
    -newattr 000; checkcfg -da kess -name BSM_FTP_WAREZ_COMPLIANT; checkcfg -da kess
    -name BSM_LOCAL_FTPD_UID
    Comment: relevant params: BSM_FTP_WAREZ_COMPLIANT BSM_LOCAL_FTPD_UID

---------------------------------------------------------------
WARNING  (41|41|11516)  BSM_DISALLOWED_FILE_EXEC   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-02-08 10:55:19.470184 PST
    Command: execve(2)   Parent_cmd: /usr/sbin/iffconfig   Outcome: 2
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 2653  sid = 2647
    Resource: /usr/sbin/iffconfig   Resource_owner: not_present
    Recommendation: killall -uname em_user1 -pid 2653 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name accesspolicy.inc
    Comment: see accesspolicy.conf

---------------------------------------------------------------
SEVERE WARNING  (42|42|11518)  BSM_DISALLOWED_FILE_EXEC   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-02-08 10:55:26.850043 PST
    Command: execve(2)   Parent_cmd: /usr/sbin/ifconfig   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 2654  sid = 2647
    Command_arg: /usr/sbin/ifconfig
    Resource: /usr/sbin/ifconfig   Resource_owner: bin
    Recommendation: killall -uname em_user1 -pid 2654 -da kess; lockout -uname em_user1
    -uid 50001 -da kess; checkcfg -da kess -name accesspolicy.inc
    Comment: see accesspolicy.conf

---------------------------------------------------------------
WARNING  (43|43|11538)  BSM_DISALLOWED_FILE_READ   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-02-08 10:55:37.079844 PST
    Command: open(2) - read   Parent_cmd: /usr/bin/cat   Outcome: 2
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 2655  sid = 2647
    Resource: /secret   Resource_owner: not_present
    Recommendation: killall -uname em_user1 -pid 2655 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name accesspolicy.inc
    Comment: see accesspolicy.conf

---------------------------------------------------------------
SEVERE WARNING  (44|44|11553)  BSM_DISALLOWED_FILE_READ   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-02-08 10:55:48.819615 PST
    Command: open(2) - read   Parent_cmd: /usr/bin/cat   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 2657  sid = 2647
    Resource: /accounting/DBMS/payroll.db   Resource_owner: em_accnt
    Recommendation: killall -uname em_user1 -pid 2657 -da kess; lockout -uname em_user1
    -da kess; checkcfg -da kess -name accesspolicy.inc
    Comment: see accesspolicy.conf

---------------------------------------------------------------
WARNING  (45|45|11794)  BSM_DISALLOWED_FILE_WRITE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-02-08 10:56:35.328695 PST
    Command: unlink(2)   Parent_cmd: /usr/bin/rm   Outcome: 13
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 2667  sid = 2647
    Resource: /accounting/DBMS/payroll.db   Resource_owner: em_accnt
    Recommendation: killall -uname em_user1 -pid 2667 -da kess; lockout -uname em_user1
    -da kess; fixperms -fn /accounting/DBMS/payroll.db -da kess -newperms 000 ; checkcfg
    -da kess -name accesspolicy.inc
    Comment: see accesspolicy.conf

---------------------------------------------------------------
SEVERE WARNING  (46|46|11840)  BSM_DISALLOWED_FILE_WRITE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-02-08 10:57:17.887843 PST
    Command: unlink(2)   Parent_cmd: /usr/bin/rm   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001  ruid = 50001  euid = 50001  pid = 2672  sid = 2647
    Resource: /accounting/DBMS/payroll.db   Resource_owner: em_accnt
    Recommendation: killall -uname em_user1 -pid 2672 -da kess; lockout -uname em_user1
    -da kess; fixperms -fn /accounting/DBMS/payroll.db -da kess -newperms 000 ; checkcfg
    -da kess -name accesspolicy.inc
    Comment: see accesspolicy.conf

---------------------------------------------------------------
WARNING  (47|47|11919)  BSM_DISALLOWED_FILE_READ   Target: kess   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-02-08 16:13:52.837138 PST
    Command: open(2) - read   Parent_cmd: /usr/sbin/in.ftpd   Outcome: 2
    Attacker: 130.107.15.118
    Attacker_attrs: auid = 0  ruid = 0  euid = 50001  pid = 2822  sid = 0
    Resource: /secret   Resource_owner: not_present
    Recommendation: kill -uname root -pid 2822 -da kess; filter -sa 130.107.15.118
    -da kess -dp 21; checkcfg -da kess -name accesspolicy.inc
    Comment: see accesspolicy.conf.  relevant params: BSM_LOCAL_FTPD_UID

---------------------------------------------------------------
SEVERE WARNING  (48|48|11920)  BSM_DISALLOWED_FILE_READ   Target: kess   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-02-08 16:14:21.076567 PST
    Command: open(2) - read   Parent_cmd: /usr/sbin/in.ftpd   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: auid = 0  ruid = 0  euid = 50001  pid = 2822  sid = 0
    Resource: /accounting/DBMS/payroll.db   Resource_owner: admin_u
    Recommendation: kill -uname root -pid 2822 -da kess; filter -sa 130.107.15.118
    -da kess -dp 21; checkcfg -da kess -name accesspolicy.inc
    Comment: see accesspolicy.conf.  relevant params: BSM_LOCAL_FTPD_UID

---------------------------------------------------------------
SEVERE WARNING  (49|49|12070)  BSM_TIME_WARP   Target: 130.107.12.70   Count: 1
    Observer: eXpert-BSM   Observer_Location: kess   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 08:11:13.118565 PST
    Command: clock   Parent_cmd: not_present   Outcome: 0
    Attacker: non_present
    Attacker_attrs: backward_drift = [1584252 seconds]
    Recommendation: diagnose -scv systime -da kess -currtime 950055325 -prevtime 948471073;
    checkcfg -da kess -name BSM_MAX_BACKWARD_TIME
    Comment: relevant params: BSM_MAX_BACKWARD_TIME


appcommon.c:251 NoDataCB(SignificantEvent):
 Interface close (idle 1009 msec) event-manager saw 12072 events, last seq # 12071,
       max idle 360000 msec


eXpert-BSM event channel closing.  PBEST shutting down.
```