HTTP://WWW.SDL.SRI.COM/INTRUSION/

EMERALD$^{(TM)}$ *eXpert-BSM*$^{(TM)}$

EMERALD Development Project

March 2000
Acknowledgments:

DARPA ITO
DARPA ISO

Sun Solaris Host-Based Intrusion Detection System

System Design Laboratory

SRI International

Release Date: March 27, 2000

User's Guide, Version 1.0

EMERALD Development Team
emerald@sdl.sri.com

Martin Fong, Ulf Lindqvist (PI), Phillip Porras (PI), Keith Skinner, Alfonso Valdes (PI),

Peter Neumann, Mike Frandsen, Sandy Smith, Lynn Voss

I Table of Contents

2. 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 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. See Section Contact and Experience Reporting Information for pointers on where to send questions, bug reports, and detected attack summaries.

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 is 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.

Your Responsibilities as an EMERALD User

There is no charge to use this application. Support for this application is very limited in that the EMERALD team is not funded to provide individual support. Special arrangements for support can be established (for further information see Contact and Experience Reporting Information). By downloading and using this prototype intrusion detection software application, you agree to the following conditions:

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

3. EMERALD *eXpert-BSM* Overview

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 realtime 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 realtime 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 statistical profile-based anomaly detection or both, on a target event stream. The statistical subsystem tracks subject activity via one of four types of statistical variables called *measures*: categorical, continuous, intensity, and event distribution. 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 known "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.

What is eXpert-BSM?

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.

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 2.5.1+ operating systems.

4. *eXpert-BSM* Detection Summary

The *eXpert-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.

Attack heuristics are assigned the following severity metrics for *eXpert-BSM:*

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

Warning-Level Heuristics

- **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 passwords submitted for a user's account. This covers I&A activity from console, telnet, and r(sh|exec) interfaces.

- **BSM_RootCore_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.

- **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 security hole allows someone to repeatedly submit user account names until a legitimate name is discovered.

- **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.

- **(Disabled in this release) BSM_AfterHours_Access: BSM Monitor provides a service to allow administrators to specify blackout hours (e.g., midnight to 6a.m.) during which certain users or groups of users are not expected or authorized to login to the host. BSM monitor will raise a warning when this after-hours access policy is violated; for more information, see Setting a Monitoring Policy**, Configuring *eXpert-BSM*.

Severe-Warning-Level Heuristics

- **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.

- **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.

- **BSM_Make_Temp_Sym**: BSM Monitor observed the creation of a "suspicious" symbolic link in `/tmp`. This is a common, even scripted, action that an intruder makes while subverting a system.

- **BSM_Mod_System_Resource**: BSM Monitor raises an alert indicator when a *nonreserved* account user alters a system resource log file. It catches attempts to modify system files in `/etc, /var/log`. This is a highly general heuristic for recognizing common actions that occur after compromise.

- **BSM_Load_MOD_SH**: BSM Monitor observed a signature for the load module (user to root) attack. Two heuristics (MOD_BIN and MOD_SH) are applied. These involve detection of certain actions on `/tmp` files.

- **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.

- **BSM_FTP_Warez_Activity**: BSM monitor observed N anonymous users retrieving an anonymously uploaded file that has been registered by BSM_FTP_Anon_Write.

- **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.

- **BSM_Proc_Exhaust_Threshold**: BSM Monitor observed process resource exhaustion. This heuristic provides a basic threshold analysis on failed fork syscalls.

- **BSM_File_Exhaust_Threshold**: BSM Monitor observed a continuing series of failed write/create operations that were rejected for lack of available filesystem space.

- **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.

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

- **BSM_Port_Sweep** [1]: Applicable to Solaris 2.6 and above. The BSM Monitor observed a port sweep from a remote host to the host audit server.

- **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.

- **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 IP address of the requester.

Attack-Level Heuristics

- **BSM_PS_Exploit**: BSM Monitor observed the execution of the PS exploit (user to root) attack.

- **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 (default = bin and sys, but could be environment specific).

- **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 that is not owned by root or the SUID user.

- **BSM_Change_User_Environ_File**: BSM Monitor observed the contents of a user's environment files (the default list = `.cshrc, .login, .rhosts, .forward, .logout`) being modified by another user. This is a highly general heuristic for recognizing common actions that occur after compromise.

- **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. This is unacceptable behavior with respect to `/etc/shadow`: `del, chmod, creat, chown, rename.`

- **BSM_Mod_System_Executable**: BSM Monitor observed the alteration of a system executable. It catches attempts to modify system binaries (default = `/bin, /usr/bin/, /usr/local/bin/, /opt/local/bin/, /usr/sbin/`). This is a highly general heuristic for recognizing common actions that occur after compromise.

- **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.

- **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_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 listed in the ADMINSTRATIVE_USER_LIST, see Configuring *eXpert-BSM*.

- **BSM_Self_Echo_Alert**: BSM Monitor observed the self-ping denial-of-service attack.

[1] - BSM network monitoring is fundamentally limited in only allowing visibility of connection requests to ports on which a process is listening. Therefore, connection requests to unused ports cannot contribute to triggering alarms for this rule.

5. System Requirements

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

- SunOS 5.5.1 (Solaris 2.5.1)
- SunOS 5.6 (Solaris 2.6), service patch 105621-19
- Solaris 7, service patch 106541-10
- Solaris 8

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

Solaris service patches may be retrieved from http://sunsolve.sun.com. For more information on the relevant Solaris kernel bugs that must be patched before running *eXpert-BSM*, see Sun Bug ID 4194454 and 4229414.

To view your machine's current patch level, use the command:

```
% /bin/showrev -p
```

6. Download Instructions

EMERALD *eXpert-BSM* is available for download to those who register 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 EMERALD 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.

We maintain the set of current release notes based on your questions and feedback regarding difficulties or problems with this distribution at

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

7. Contents of Distribution

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

```
doc                      Documentation directory
   user-manual_1_0.pdf   This user document
   COPYRIGHT             EMERALD copyright information


_BSM                     EMERALD executable directory
   Install_eXpert_BSM    Installation script (run as root)
   Run_eXpert_BSM        Startup script
   Shutdown_eXpert_BSM   Shutdown script
    Start_GUI            Alert Management Interface script
   _resolver_to_ascii    Convert resolver files to ASCII
   _bsm_to_ascii         Convert BSM file to ASCII
   eXpert-config.sh      Run parameters for Run_eXpert_BSM


bin                      Solaris 2.5.1 thru 2.8 bins
  SunOS-5.*              EMERALD executables directory
   ask_yn                Utility script
   ebsmgen               BSM-to-EMERALD data converter
   ebsmprobe             Realtime BSM data retrieval
   emsgdump              Results file dump utility
   eXpert-BSM            EMERALD expert-system BSM analyzer
   slay                  Utility script
   throttle              I/O buffering process


resource-object
   pfull.tmpl            EMERALD resource-object directory
   report.tmpl           Event definition in EMERALD format
   audit_config.tar      EMERALD results definition
   eXpert.init           Tar file of audit-configuration
   emsg-BSM.init         BSM expert-system resource object
   ebsmgen.init          Results-file dump resource object
   config
     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
```

_BSM/results	*Results and log directory*
bsm-alerts-.resolver	*EMERALD format alerts file*
bsm-alerts-*.ascii	*ASCII alerts file*
bsm-expert-*.log	*eXpert-BSM error log*
bsm-generatr-*.log	*BSM data converter log*
idip-message*.log	*Optional IDIP alert log*
gui	*This directory contains the*
*	*EMERALD JAVA 1.1.8 GUI subsystem*
samples	*An extensive battery of BSM records (encoded in EMERALD binary format)*
eXpert-battery.ebin	*that exercise the eXpert-BSM knowledge-base*

8. Pre-Installation Cautions and Caveats

What You Need Before Installation

- Root privilege is required to Install *eXpert-BSM* for realtime 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 *eXpert-BSM* on the target host's local hard drive rather than an NFS mounted partition when operating this system in realtime mode.
- The Solaris 2.6 and Solaris 7 operating systems require certain service patches set from Sun Microsystems (see below).
- We strongly recommend that *eXpert-BSM* be installed when no other users are using the target host.

Caution: Solaris Bugs

If you are attempting to install *eXpert-BSM* on Solaris 2.6, Solaris 7, 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 for information on bugs and patches.

Sun Bug ID	Description	Possible Patch
4194454	auditing to pipe causes system to panic	105621-19 (5.6) 106541-10 (5.7)
4229414	Solaris 7 64 bit BSM auditing with +argv policy break exec()	106541-10 (5.7)

9. Installing *eXpert-BSM*

Solaris Audit Installation

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 and bring the system into 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
```

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+ 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 EMERALD process chain. We recommend the following setup strategy (advisory only, not required):

1. Create an exclusive account for running the EMERALD BSM monitor, called `emerald`.
2. Extract the EMERALD Monitor 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 EMERALD 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 EMERALD. 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 a Solaris 2.5.1+. If it is not, the following message appears:

```
===========================================================
Unsupported operating system: $os_name
This version of the EMERALD BSM Monitor is designed for"
Solaris 2.5.1+
```

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

```
============================================================
EMERALD BSM monitor installation: $tmstamp

*********************************************************
*                                                       *
*                      EMERALD (tm)                     *
*         copyright 1997-2000 SRI International         *
*                                                       *
*   This is an UNPUBLISHED work of SRI International    *
*   and is not to be used, copied or disclosed except   *
*   as provided in the License Agreement with SRI       *
*   International.                                      *
*                                                       *
*   EMERALD is a Trademark of SRI International         *
*                                                       *
*********************************************************

 Attention: You are about to install the EMERALD (TM) BSM Monitor
 intrusion detection monitor into your system.  This component
 is designed for a Solaris 2.5.1+ operating system 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.
```

3. `Install_eXpert_BSM` verifies that you are operating as user root. Root is required to modify the audit configuration and enable realtime access to kernel audit data.

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

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

If you wish to employ *eXpert-BSM* for realtime 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.

4. 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
```

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

5. `username_map.conf` is automatically generated by the installation script and provides EMERALD with a mapping between Subject IDs and human-readable usernames. Later additions to this file may be made with a text editor should you add or delete user accounts after installing *eXpert-BSM*. This map allows EMERALD 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
      smtp      0
      uucp      5
      nuucp     9
      listen    37
      operator  28
      johnny    443
      suzie     445
```

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

```
============================================================
The EMERALD BSM monitor 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 EMERALD will be operated under the emerald group, then type `emerald.`

```
Enter the group name or username that will be allowed
to run the BSM monitor (e.g., emerald):
```

8. EMERALD determines if the audit daemon is currently running. If it is, you are prompted as follows:

```
============================================================
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. EMERALD determines whether the audit subsystem is currently enabled on your system. The audit subsystem should not be enabled; *eXpert-BSM* does not work in parallel with the Solaris audit daemon. Type 'Y' to continue with the installation process. To later re-enable Solaris auditing, simply rename the file `audit_startup.renamed_by_emerald` file to `audit_startup`.

```
EMERALD 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. EMERALD attempts to install a custom audit configuration.

```
============================================================
The EMERALD BSM monitor 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 EMERALD configuration is installed.
```

10b. EMERALD 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${tmstamp}.tar`.

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

10c. EMERALD 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.

```
============================================================
The files
  /etc/security/audit_event /etc/security/audit_startup
  /etc/security/audit_user /etc/security/audit_warn
  /etc/security/audit_data
will be deleted.

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

11. EMERALD unloads and installs the following files into /etc/security/:

```
     audit_event
     audit_startup (a script)
     audit_user
     audit_warn
     audit_data
```

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.

```
============================================================
If you wish to run EMERALD now, then allow this script to
configure the audit collection policy, otherwise please
reboot host before starting EMERALD.

Configure audit policy now (Y/N)?
```

13. *eXpert-BSM* provides a Java-based Alert Management Interface for managing intrusion alerts. The Alert Management Interface requires the **JAVA 1.1.8 JDK.**

```
============================================================
The EMERALD GUI requires the use of the JAVA
Development Kit (JDK), which must be installed on your
system and accessible to the account from which you
will run EMERALD.  The JDK can be obtained from Sun
Microsystems at http://www.sun.com/solaris/java.  If
you decline to configure EMERALD for the JDK now, but
```

```
later wish to use the EMERALD GUI, you may run this
installation script again and configure the JDK.

Do you wish to enable the EMERALD GUI (y/n)?
```

Type 'Y' if you have the Java 1.1.8 JDK installed and you know its directory path.

```
Please type the full directory path of the
JDK (e.g., /bin/java-1.1/):
```

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

```
EMERALD monitor installation complete.
```

10. Configuring *eXpert-BSM*

eXpert-BSM provides an unprecedented degree of 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 Section 9, you must perform the *eXpert-BSM* configuration phase. While we provide the most generally applicable defaults, 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 *eXpert-BSM*.
- Configuring the Local Network Address List: provides *eXpert-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 *eXpert-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`.

- 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. 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"`**

- SETTING IDIP ALERT MODE: *eXpert-BSM* can produce an IDIP message as specified by the Boeing *Intrusion Detection Internet Protocol*. To produce these messages, set this variable to "on";"off" is the default. For more information on IDIP, see Contact and Experience Reporting Information.

  - **`set IDIP_ALERT_MODE = "off"`**

- ENABLING SOCKETS VS UNNAMED PIPES: This switch tells *eXpert-BSM* that its components will use Internet sockets as the primary data stream transport. Default = "yes", which indicates that components will not use unnamed pipes for communication channels. This option applies only to realtime operation.

  - **`set USE_SOCKETS = "yes"`**

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 following are available for knowledge-base customization:

- 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 *eXpert-BSM* who the current list of users are that may legally acquire root control.
- Default: None. You must specify.

```
MsgString BSM_ADMINISTRATIVE_USER_LIST {  }
```

- 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

```
MsgString BSM_USER_ENV_FILES  {.cshrc .forward
.rhosts  .login .logout}
```

- 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: /export/home/

```
Char BSM_USER_HOMES_LOCATION = /export/home/
```

- 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/, /etc/

```
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
}
```

- 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 logins.
- 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_RESTRICTED_HOURS_ULIST
- Dependent Rules: BSM_AfterHours_Access
- Purpose: Indicates the list of user or group names subject to the restricted login hours (bad login hours are specified using RESTRICTED_HOURS_START /STOP variables).
- Default: Empty list of usernames and group names.

```
MsgString BSM_RESTRICTED_HOURS_ULIST   { }
```

- Parameter: BSM_RESTRICTED_HOURS_START
- Parameter: BSM_RESTRICTED_HOURS_STOP
- Dependent Rules: BSM_AfterHours_Access
- Purpose: Indicates periods of time in which the lists of restricted users or groups are restricted from logins to the host. If BSM_RESTRICTED_HOURS_ULIST (above) is empty, this rule is effectively disabled.
- Default: 23:00:00 (in 24hr notation, local time)

```
Char BSM_RESTRICTED_HOURS_START =  23:00:00
Char BSM_RESTRICTED_HOURS_STOP  =  04:30:00
```

- 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 user-names 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_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_Read_Private_File, BSM_Write_Private_File, BSM_Illegal_Execution, BSM_Promiscuous_Mode, BSM_Mod_System_Executable.
- 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_Make_Temp_Sym
```

```
       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_Read_Private_File
       BSM_Write_Private_File
       BSM_Illegal_Execution
       BSM_Promiscuous_Mode
       BSM_Self_Echo_Alert
     }
```

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 <subnet_mask>
or
       host <ip_address>
```

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.

There are three distinct components to be specified within an EMERALD 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_A{
               nread [ file_list_A file_list_B ... ]
               nwrite[ file_list_C file_list_D ... ]
               nexec [ file_list_E file_list_F ... ]
       }
       user_list_B{
               nread [ file_list_A file_list_B ... ]
               nwrite[ file_list_C file_list_D ... ]
               nexec [ file_list_E file_list_F ... ]
       }
       ...
}
```

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 PayrollData]
                   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 writes 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 are 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.

11. Operating Instructions

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

```
$Install/_BSM/Run_eXpert_BSM

Usage:  Run_eXpert_BSM [ -TEST ]
         or Run_eXpert_BSM [ bsm_file [-L] ]
         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
               LIVE-FILE - bsm file and -L option set
```

Realtime: 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 saves those records representing malicious activity. However, follow the caveats in this file for restarting the operating system after *eXpert-BSM* is shut down. 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 is `$Install/samples/emerald-attack-battery.ebin`.

```
% 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 EMERALD run directory (`$Install/_BSM`) and execute the following command

```
% Run_eXpert_BSM  <BSM_Audit_File>
```

Live Audit File Processing: *eXpert-BSM* can be run in coexistence with the Solaris Audit daemon by reading the live audit file as the file is being written by the audit daemon. This allows the site to maintain permanent audit logs of all data sets, while still supporting EMERALD's realtime analysis capability.

Instructions:

1. Using ps, verify that audit process `/usr/sbin/auditd` is running.

2. Get the name of the current audit file by examining file /`etc/security/audit_data`. For example, this file will contain a line similar to the following:

```
239:/var/audit/19990602185407.not_terminated.host
```

where /`var/audit/19990602185407.not_terminated.host` represents the name of the current audit file being written by `/usr/sbin/auditd` on the `host` machine.

3. As root, you will need setup group permission access to the audit file for the user who will be operating the EMERALD monitor. We recommend an IDS group that is allowed read access to files in `/var/audit`.

4. To begin analysis, move to the EMERALD bin directory `($Install/_BSM`) and execute the following command

```
%Run_eXpert_BSM /var/audit/1999060218540.not_terminated.host -L
```

To determine whether the monitor has started successfully, move to the results directory and review the log files `($Install/_BSM/results`). Diagnostic errors will be produced in either file bsm-expert-*.log or bsm-generator-*.log.

The *eXpert-BSM* Process Chain

Run_eXpert_BSM is a csh script that invokes the following programs

- `ebsmsetpolicy` - (realtime mode) establishes an optimized audit configuration with the kernel. This is a setuid utility. It exits immediately after setting the audit configuration.
- `ebsmprobe` - (realtime 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 sigterm or `sighup`.
- `throttle` - (realtime 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.
- `ebsmgen` - (all modes) accepts Solaris BSM audit records, and converts and forwards them as EMERALD message to *eXpert-BSM*.
- `eXpert-BSM` - (all modes) is the EMERALD forward-chaining expert system.

12. Shutdown Instructions

Login under the IDS account or root and invoke

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

This script kills the process chain for the EMERALD BSM component. In realtime mode, this script kills ebsmprobe, throttle, ebsmgen, and *eXpert-BSM* in that order.

CAUTION: When running in realtime 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). 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.

13. Uninstalling *eXpert-BSM*

The EMERALD *eXpert-BSM* monitor can be safely uninstalled as follows:

1. If *eXpert-BSM* is currently running, shut it down before attempting to uninstall this component.
2. Remove the *eXpert-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`.

14. *eXpert-BSM* Report Formats

The EMERALD *eXpert-BSM* monitor produces three forms of intrusion reports: console alert, EMERALD GUI 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, as discussed in Section *eXpert-BSM* Detection Summary). 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 realtime 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.

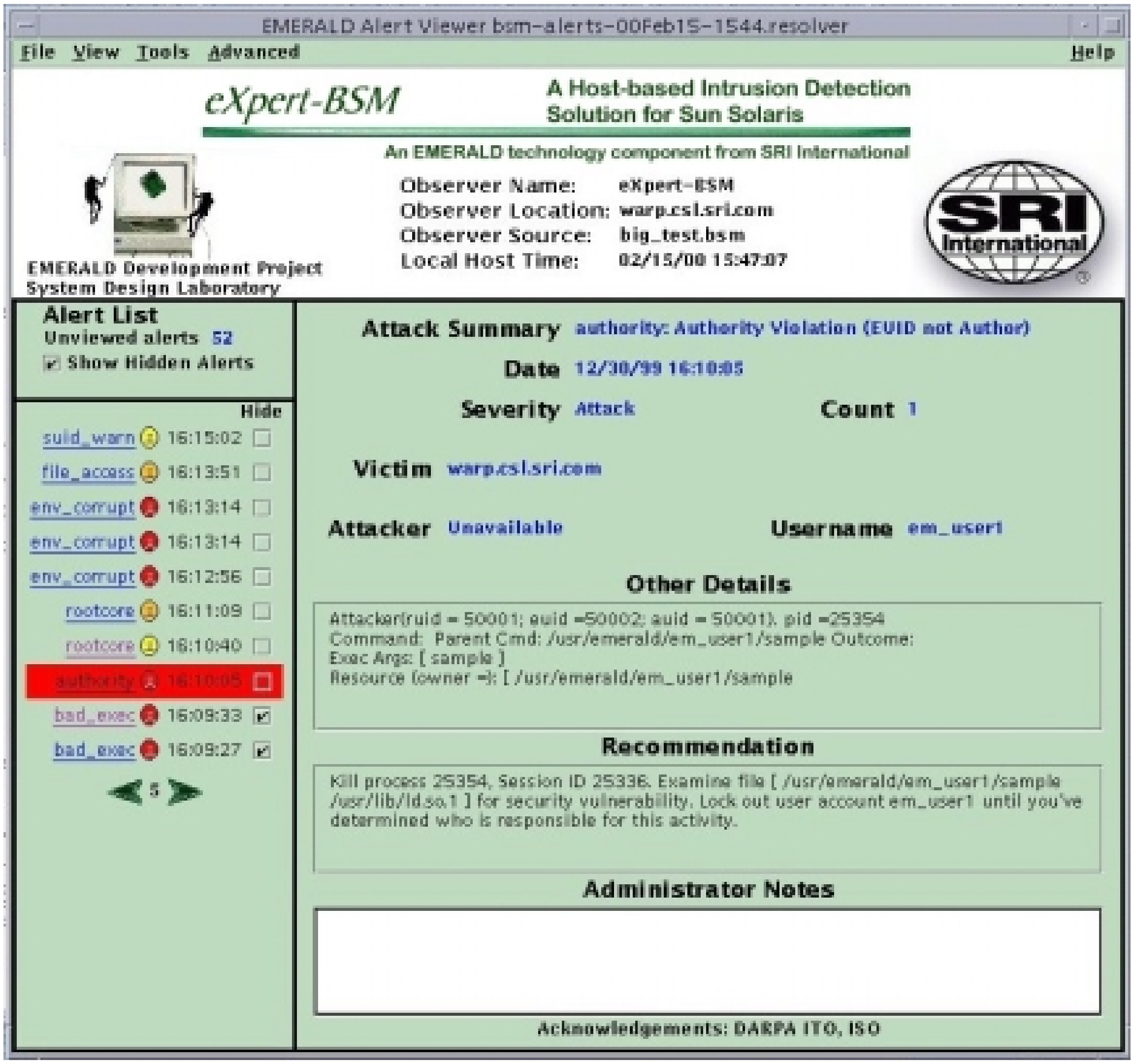
Line 9: (optional) provides recommended countermeasure directives for responding to intrusive activities. *eXpert-BSM* employs

- `KILL <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.
- `ISOLATE <filename> ---` move this indicated file to an isolated directory that cannot be accessed by non-administrative users. Disable attributes and examine contents soon.
- `FILTER <IP address> ---` if a firewall is available, disallow network connectivity from this indicated IP address.
- `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 Alert Management Interface

EMERALD provides a unique graphical user interface, shown in Figure 1, 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. This alert management interface provides a session history that allows the security administrator to maintain a record of which alerts have and have not been acted upon. Administrators can also associate incident handling notes with each alert record to document information gathered during an investigation of the alert.


EMERALD Alert Viewer bsm-alerts-00Feb15-1544.resolver
File View Tools Advanced
Help
eXpert-BSM
A Host-based Intrusion Detection Solution for Sun Solaris
An EMERALD technology component from SRI International
EMERALD Development Project
System Design Laboratory
SRI International

Observer Name: eXpert-BSM
Observer Location: warp.csl.sri.com
Observer Source: big_test.bsm
Local Host Time: 02/15/00 15:47:07

Alert List
Unviewed alerts 52
☑ Show Hidden Alerts

		Hide
suid_warn	16:15:02	□
file_access	16:13:51	□
env_corrupt	16:13:14	□
env_corrupt	16:13:14	□
env_corrupt	16:12:56	□
rootcore	16:11:09	□
rootcore	16:10:40	□
authority	16:10:05	□
bad_exec	16:09:33	☑
bad_exec	16:09:27	☑

Attack Summary authority: Authority Violation (EUID not Author)
Date 12/30/99 16:10:05
Severity Attack
Count 1
Victim warp.csl.sri.com
Attacker Unavailable
Username em_user1

Other Details

Attacker(ruid = 50001; euid =50002; auid = 50001), pid =25354
Command: Parent Cmd: /usr/emerald/em_user1/sample Outcome:
Exec Args: [sample]
Resource (owner =): [/usr/emerald/em_user1/sample

Recommendation

Kill process 25354, Session ID 25336. Examine file [/usr/emerald/em_user1/sample /usr/lib/ld.so.1] for security vulnerability. Lock out user account em_user1 until you've determined who is responsible for this activity.

Administrator Notes

Acknowledgements: DARPA ITO, ISO

Figure 1: EMERALD Alert Manager Main Window

Main Window Pull-down Menu

At the top of the Main Window is a pull-down menu bar consisting of five menus: File, View, Tools, Advanced, and Help.

FILE Menu: The File menu contains two options: Open (optional) and Exit. Open is used to start reading from another log file of attack data. Exit closes down the GUI. When exiting, three options are available: Just Exit, Exit and remove this History, and Exit and Remove All Histories. Just Exit closes down the GUI without deleting the persistent history files of this alert log on the disk. Exit and Remove This History shuts down the GUI and deletes any persistent files associated with the currently read attack data, but not the original attack data file itself. Exit and Remove All Histories closes down the GUI and deletes all persistent files associated with running the GUI for all attack data read, but does not delete the original attack data files themselves.

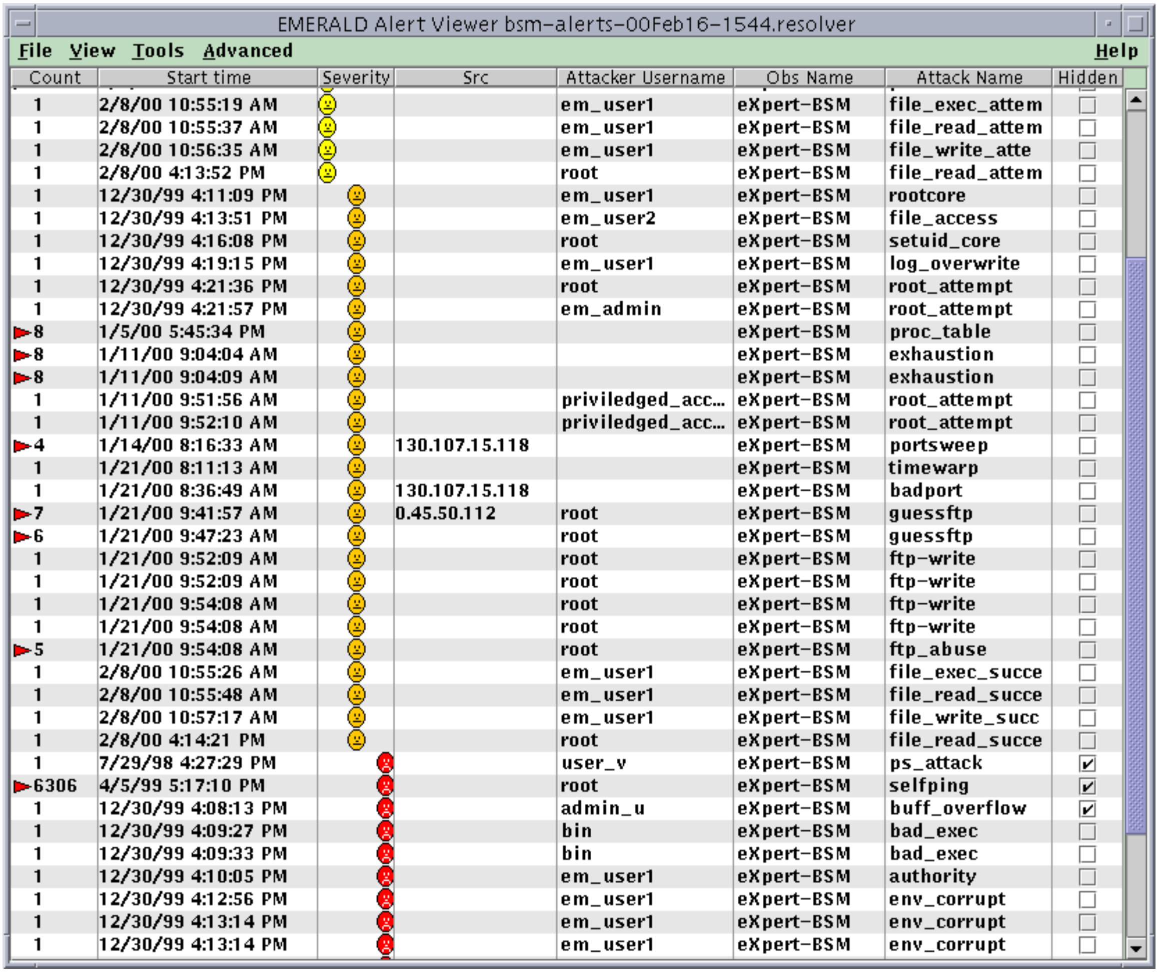
View Menu: The View menu provides five options: Main View, Table, Table Configuration, Do IP-Name Lookup, and TimeZone setting. Main View causes the GUI to display the Main Window shown in Figure 1. Table displays all alerts in a tabular form, as illustrated in Figure 2, with one attack listed per table row. The columns display the various fields in the attack. The rows can be sorted according to a particular field by clicking on the column label at the top of the column. To reverse sort a field, you may right-click on the column header with your mouse. Columns can be re-ordered by clicking on the column header and dragging it to a new location. Note: the Hidden column is not the same as the Hide feature of the main view. Thus, selecting Hidden on the table does not hide alerts in the alert list and selecting Hide in the main view's alert list does not hide rows in the table. Selecting Table Configuration allows you to configure the columns and sorting strategy for the Table view. Do IP-Name Lookup toggles the Main View window between displaying host IP addresses in Internet dot notation or symbolic names. The TimeZone item allows you to select from 32 distinct timezone formats for displaying alert timestamps.

Tools Menu: The Tools menu has four options: Email, Print, Respond, and Search. Email brings up the currently selected alert description in a new window and allows the GUI operator to send an email message off to any valid email address. Email is described in more detail near the end of this document. Print sends the currently selected alert to the default installed printer connected to your computer, if one exists. If no printer is installed or properly configured this feature does not work. Currently, the Respond and Search features are not implemented.

Advanced Menu: The Advanced menu has three options: All Alerts , Email Preferences, and Auto-Hide. All Alerts has three options: Set Viewed marks all the currently available alerts as viewed, thus displaying them with purple text; Set Hide hides all alerts in the Alert List as described below; Auto-Hide provides filtering criteria that allow you to specify whether incoming alerts should set automatically to hidden. Using the Auto-

Hide feature, one can filter incoming alerts by alert name, observer name, or by severity level. Email Preferences has two options: Set Sender allows the user to configure who is operating the GUI and thus who is sending the email; Set SMTP Server allows the operator to set a new mail server if the one set in the ".config" file is not valid.

Help Menu: The Help menu has two options: Using Alert Viewer provides a brief description of this alert management interface, and About shows the current EMERALD copyright information.



Count	Start time	Severity	Src	Attacker Username	Obs Name	Attack Name	Hidden
1	2/8/00 10:55:19 AM	🟡		em_user1	eXpert-BSM	file_exec_attem	□
1	2/8/00 10:55:37 AM	🟡		em_user1	eXpert-BSM	file_read_attem	□
1	2/8/00 10:56:35 AM	🟡		em_user1	eXpert-BSM	file_write_atte	□
1	2/8/00 4:13:52 PM	🟡		root	eXpert-BSM	file_read_attem	□
1	12/30/99 4:11:09 PM	🟠		em_user1	eXpert-BSM	rootcore	□
1	12/30/99 4:13:51 PM	🟠		em_user2	eXpert-BSM	file_access	□
1	12/30/99 4:16:08 PM	🟠		root	eXpert-BSM	setuid_core	□
1	12/30/99 4:19:15 PM	🟠		em_user1	eXpert-BSM	log_overwrite	□
1	12/30/99 4:21:36 PM	🟠		root	eXpert-BSM	root_attempt	□
1	12/30/99 4:21:57 PM	🟠		em_admin	eXpert-BSM	root_attempt	□
►8	1/5/00 5:45:34 PM	🟠			eXpert-BSM	proc_table	□
►8	1/11/00 9:04:04 AM	🟠			eXpert-BSM	exhaustion	□
►8	1/11/00 9:04:09 AM	🟠			eXpert-BSM	exhaustion	□
1	1/11/00 9:51:56 AM	🟠		priviledged_acc…	eXpert-BSM	root_attempt	□
1	1/11/00 9:52:10 AM	🟠		priviledged_acc…	eXpert-BSM	root_attempt	□
►4	1/14/00 8:16:33 AM	🟠	130.107.15.118		eXpert-BSM	portsweep	□
1	1/21/00 8:11:13 AM	🟠			eXpert-BSM	timewarp	□
1	1/21/00 8:36:49 AM	🟠	130.107.15.118		eXpert-BSM	badport	□
►7	1/21/00 9:41:57 AM	🟠	0.45.50.112	root	eXpert-BSM	guessftp	□
►6	1/21/00 9:47:23 AM	🟠		root	eXpert-BSM	guessftp	□
1	1/21/00 9:52:09 AM	🟠		root	eXpert-BSM	ftp-write	□
1	1/21/00 9:52:09 AM	🟠		root	eXpert-BSM	ftp-write	□
1	1/21/00 9:54:08 AM	🟠		root	eXpert-BSM	ftp-write	□
1	1/21/00 9:54:08 AM	🟠		root	eXpert-BSM	ftp-write	□
►5	1/21/00 9:54:08 AM	🟠		root	eXpert-BSM	ftp_abuse	□
1	2/8/00 10:55:26 AM	🟠		em_user1	eXpert-BSM	file_exec_succe	□
1	2/8/00 10:55:48 AM	🟠		em_user1	eXpert-BSM	file_read_succe	□
1	2/8/00 10:57:17 AM	🟠		em_user1	eXpert-BSM	file_write_succ	□
1	2/8/00 4:14:21 PM	🟠		root	eXpert-BSM	file_read_succe	□
1	7/29/98 4:27:29 PM	🔴		user_v	eXpert-BSM	ps_attack	☑
►6306	4/5/99 5:17:10 PM	🔴		root	eXpert-BSM	selfping	☑
1	12/30/99 4:08:13 PM	🔴		admin_u	eXpert-BSM	buff_overflow	☑
1	12/30/99 4:09:27 PM	🔴		bin	eXpert-BSM	bad_exec	□
1	12/30/99 4:09:33 PM	🔴		bin	eXpert-BSM	bad_exec	□
1	12/30/99 4:10:05 PM	🔴		em_user1	eXpert-BSM	authority	□
1	12/30/99 4:12:56 PM	🔴		em_user1	eXpert-BSM	env_corrupt	□
1	12/30/99 4:13:14 PM	🔴		em_user1	eXpert-BSM	env_corrupt	□
1	12/30/99 4:13:14 PM	🔴		em_user1	eXpert-BSM	env_corrupt	□

Figure 2: EMERALD Alert Manager Table View

Main Window View

Title Panel:

The Title panel is the top horizontal panel of the Main View window, and contains the alert management interface title with the EMERALD and SRI International logos. In the middle of the Title panel are four fields: Observer Name, Observer Location, Local Host

Time, and Observer Source. Local Host Time is the current time on the host running the GUI updated every second. The other three fields are present only when an alert in the alert list is highlighted (the procedure to select an alert is explained below).

Alert List Panel:

The Alert List panel is on the far left of the GUI below the title panel described above. In the top box of the alert list is the number of unviewed and viewable alerts. An alert is considered unviewed until the user selects it from the list of alerts below and has the alert's information displayed in the bottom right panel or until the user chooses Set Viewed from the Advanced menu. Viewable alerts are alerts that do not have their associated hidden flag set. Below the number of viewable alerts is a checkbox labeled: Show Hidden Alerts. If this is checked, all alerts that have been previously hidden are added to the list of alerts in the panel below. If this is not checked, only alerts which have not been hidden are displayed in the list below. In the space below the Show Hidden Alerts checkbox is room for a message which is not always visible. This message (in red font when visible) displays the number of alerts that have arrived into the GUI since the user last selected an alert for viewing. This message allows the user to keep track of new alerts when the GUI is left unattended. Below the alert list is a series of tabs containing the actual alerts. Each alert appears on a separate line that contains the alert name, a severity icon, and the timestamp indicating when the alert was generated. To select an alert, click on either the attack name or the severity icon. Once an alert is selected, its row is highlighted with a red box and its information is displayed in the Alert Description panel. As alerts are selected, their names change in color from blue to purple, similar to the color scheme of most web browsers.

The severity icon represents four possible levels of severity for alerts:

- Informative - Green smiley face
- Warning - Yellow face
- Severe Warning - Orange face
- Attack - Red frowning face

By default, the Alert List panel will display up to ten alerts. Two arrow buttons at the bottom of this panel are provided to switch between alert sets. The number between the two arrow buttons indicates the number of additional Alert List panels available. The arrow buttons are "grayed out" when there no additional alerts to view.

Alert Description Panel (center panel displaying alert content)

When one of the alerts are selected in the alert list describe above, this panel is filled out with the information present in the currently selected alert. At the top of this panel are the Attack Summary, Date, Severity, Count, Update, Victim, Attacker, and Username fields. The Attack Summary line contains the name of the attack followed by a colon and a short description of the attack. The Date line contains the starting time of the attack. If the attack spanned a period of time, it also contains the ending time of the attack. The Severity field contains the level of severity this attack represents in words corresponding to the icon displayed in the alert list panel. The Count represents the number of individual occurrences of the malicious phenomena encountered by the intrusion detection tool. The Update field represents the number of *common* alerts that have been automatically merged by the Alert Management Interface. EMERALD sensors have the ability to produce multiple alerts regarding a single intrusion incident, providing additional information during the duration of an attack. These alerts are associated under a single reporting *thread*; this common thread is recognized and automatically merged by the Alert Management Interface.

Victim shows the host name of the computer being attacked or the IP address (use the View menu Do IP-Name Lookup feature to toggle between IP and symbolic host name displays). If multiple computers were attacked then "multiple" is displayed. Attacker shows the host name of the computer that initiated this attack if known, otherwise "Unavailable" is displayed. The Username field contains the attacker's username, if known.

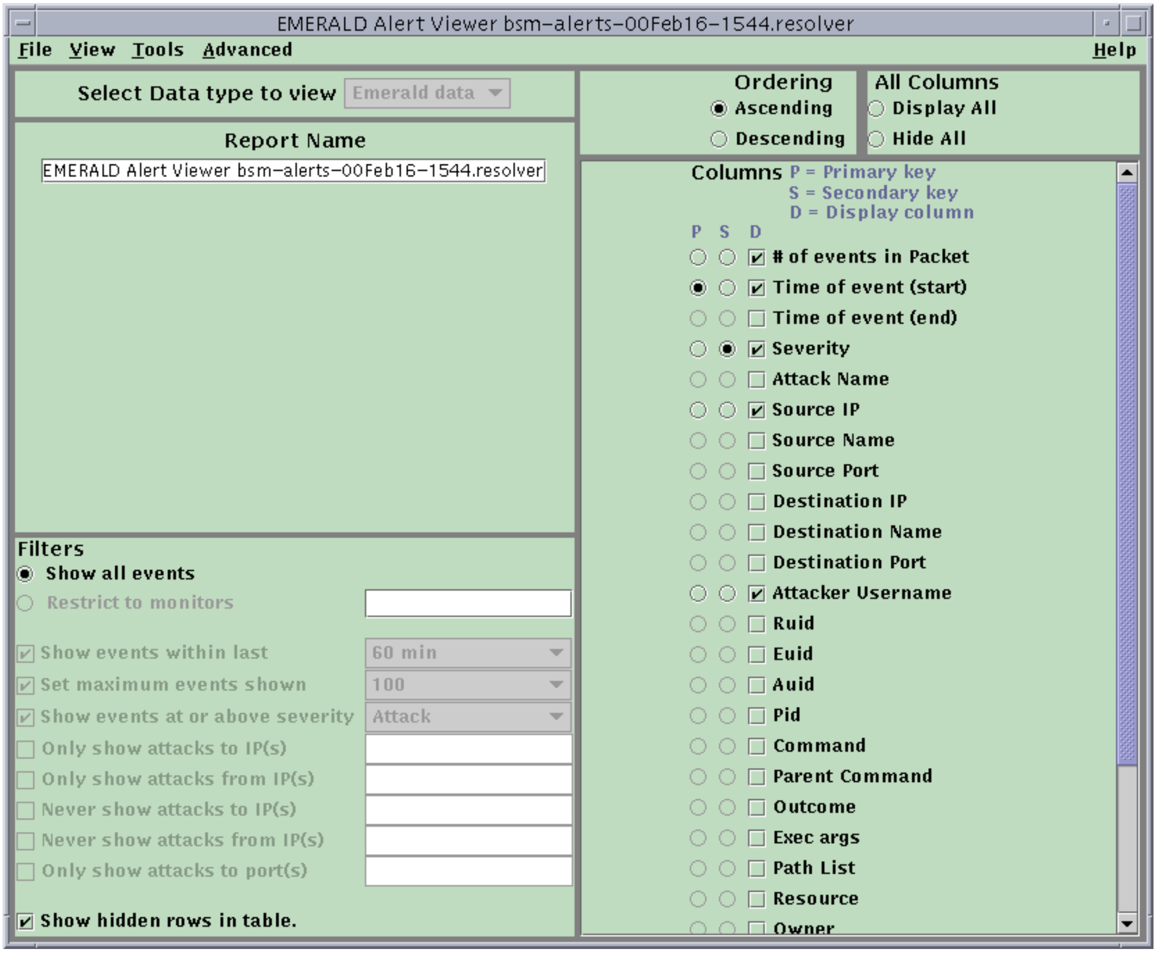
The Other Details section displays other information known about the alert depending on the attack type. The attacker's ruid, euid, auid, or pid information is displayed, if available. If the attacker's command or parent command are known, they are displayed. If the alert pertains to an execution event, its arguments are shown on the next line. If the attack involves manipulation of a resource, the resource pathname and owner are shown.

Below the "Other Details" section is the "Recommendation" section. This section contains text explaining optimal countermeasures that should be performed to counter the intrusive activity.

At the bottom of the Alert Description panel is the "Administrator Notes" area. This section provides an area to record incident handling notes associated with the alert investigation. These notes are stored in a history file associated with the alert report, providing a permanent record of annotations that may be shared with the security staff as EMERALD reports are processed.

Alert Table Configurations

Selecting Table Configuration, shown in Figure 3, from the View menu allows the GUI operator to customize the look of the table. In the top left corner is the data type to view. Currently only Emerald Data is allowed so this option is not selectable. In the center-left region is the name of this report. Changing the name in the label will change the title displayed for this EMERALD Alert Viewer window the next time the table is displayed. In the bottom-left corner are various filters for screening which rows should be displayed in the table. Currently the only configurable option is the last one: Show Hidden Rows in Table. If this is selected, all rows are displayed in the table. If it is not selected (default), hidden rows are not displayed in the table. In the upper center region is the Ordering option, which allows ascending and descending ordering. In the upper right corner are the options for displaying or hiding all columns, which select or unselect the Display column checkboxes in the lower right corner. In the lower right corner are the Columns, which can be displayed in the table view. For each column the user can choose whether the column should be displayed or not with the checkbox in the "D" column. Columns are sorted based on both a primary key "P" and a secondary key "S". The primary key should be selected first, which will allow the rows to be ordered by the data in this column. The secondary key should be selected next, which allows the rows to be further sorted by the data in this column when data in the primary key field is equal.



Select Data type to view: Emerald data

Report Name: EMERALD Alert Viewer bsm-alerts-00Feb16-1544.resolver

Filters
● Show all events
○ Restrict to monitors
☑ Show events within last: 60 min
☑ Set maximum events shown: 100
☑ Show events at or above severity: Attack
□ Only show attacks to IP(s)
□ Only show attacks from IP(s)
□ Never show attacks to IP(s)
□ Never show attacks from IP(s)
□ Only show attacks to port(s)
☑ Show hidden rows in table.

Ordering
● Ascending
○ Descending

All Columns
○ Display All
○ Hide All

Columns P = Primary key
S = Secondary key
D = Display column

P	S	D	
○	○	☑	# of events in Packet
●	○	☑	Time of event (start)
○	○	□	Time of event (end)
○	●	☑	Severity
○	○	□	Attack Name
○	○	☑	Source IP
○	○	□	Source Name
○	○	□	Source Port
○	○	□	Destination IP
○	○	□	Destination Name
○	○	□	Destination Port
○	○	☑	Attacker Username
○	○	□	Ruid
○	○	□	Euid
○	○	□	Auid
○	○	□	Pid
○	○	□	Command
○	○	□	Parent Command
○	○	□	Outcome
○	○	□	Exec args
○	○	□	Path List
○	○	□	Resource
○	○	□	Owner

Figure 3: Table Configuration View

Miscellaneous Features

Printing: Once an alert has been selected and its information is displayed in the bottom right panel, the user can choose to print it to have a hard copy of this information. If the user presses print and the computer running the GUI has a printer installed on it locally or available on the network, the contents of the GUI is printed to that printer. If no printer is installed or properly configured, this feature will not work.

Email: Also, once an alert has been selected, it can be emailed to anyone. For this feature to work properly, the operator must have edited the ".config" file prior to running the

GUI. In the ".config" file are two lines one for SMTPServer which must be set to a valid SMTP server. The other line is for MailSender which should be set to the email address of the person monitoring the GUI but can be set right before the email message is sent. After an alert has been selected, the user can press the Email button in the title panel. A popup will be displayed with a default subject line and a message containing the contents of the GUI's current alert. The To line must be filled in with the email address of the person whom this message should be sent to. The subject and message contents itself are both editable and can be modified or added to prior to pressing the Ok button on the email popup to send the message. If the Cancel button is pressed first, the message is not sent and the user is returned to the original GUI display.

Handling Multiple ID Components Under Single Alert Manager: EMERALD does support the simultaneous management of multiple EMERALD components distributed across multiple hosts. For example, a single Alert Management Interface can provide realtime management of multiple *eXpert-BSM* Monitors deployed across an administrative domain. However, this feature is not provided under this release and only available under special support arrangement. See Contact and Reporting Information for more information on obtaining special support arrangements.

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
```

The console alerts produced from the EMERALD host-based attack battery are available for review in file $Install/doc/sensor-output.html.

A full test description of the EMERALD host-based attack battery is available in file $Install/doc/test-description.html.

If you would like to properly configure EMERALD *eXpert-BSM* to run against the DARPA-sponsored MIT Lincoln Laboratory Intrusion Detection Evaluation Datasets, please send an email request to emerald-support@sdl.sri.com. Note: this data set is not publically available; if you do not have access to this dataset, we cannot give it to you.

Remember that when testing *eXpert-BSM*, 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).

16. 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.

_____ YES, I agree to the following provisions as a condition precedent to my possession and use of the *eXpert-BSM*, pre-release software program Solaris Host-Based Intrusion Detection System (the "Program"). Your clicking of this box constitutes an electronic signature and is recognized as such by SRI International ("SRI") and further is made pursuant 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 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 CONSEQUENTIAL 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 one hundred and twenty (120) days after downloading the Program. Subsequent one hundred and twenty (120) day periods under this license may be granted 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 Reporting and Feedback Agreement).

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.

17. Reporting and Feedback Agreement

EMERALD *eXpert-BSM* is made available for your use in the spirit of free software development and DARPA ITO and ISO technology transfer 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 monitor. 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 that 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 revisions of *eXpert-BSM*.
3. Tell us of any documentation errors, script failures, or system errors that you experience using this package. We apologize in advance for any trouble you may have with this software.

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

18. Contact and Experience Reporting Information

If you experience problems or locate a problem in this distribution, 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 are not funded to support this free prototype release, so we regret that individual responses to your problem reports are not always possible. For other questions regarding the EMERALD project and the availability of its components for specialized purposes, you may contact the EMERALD Program Director, Phil Porras, at porras@sdl.sri.com.

For users requiring technical support for this component, direct all questions regarding **Special-arrangement Support Agreements** to emerald-support@sdl.sri.com.

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

For more information about the Intrusion Detection Internet Protocol (IDIP), contact Daniel Schnackenberg at the Boeing Information, Space, and Defense Systems Division, daniel.d.schnackenberg@boeing.com.

19. 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

20. Version Status

EMERALD *eXpert-BSM*, Version 1.0, March 27, 2000. 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.

EMERALD Alert Management Interface, Version 1.0, March 27, 2000

EMERALD User's Guide, Version 1.0, March 27, 2000

Appendix I

EMERALD eXpert-BSM
Attack Battery Test Description

EMERALD Development Project
January 2000
System Design Laboratory
SRI International

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

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 number= -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 number= -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 number= -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 number= -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>   Outcome:
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 disal-
lowed

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

EMERALD eXpert-BSM
Console Alerts
Host-IDS Attack Battery

EMERALD Development Project
January 2000
System Design Laboratory
SRI International

```
PBEST runtime library built Wed Oct 6 09:56:34 PDT 1999
User Map [/usr/emerald/Emerald_BSM_EXPERT_Apr2000/resource-object/config-
TEST/username_map.conf] Loaded Successfully

--------------------------------------------------------------
EMERALD Control Protocol eXpert, Real-Time, 0.02
An unpublished work of SRI International
Computer Science Laboratory, SRI International, January 1999
All Rights Reserved. EMERALD (tm) Trademark SRI International.

Direct all comments or questions to: emerald@csl.sri.com

Monitor Started: Mon Apr 10 16:20:40 2000

Operating from:
    Hostname: tuvok
    IP Address: 130.107.12.102
    Report Log: <STDOUT>
--------------------------------------------------------------

Loading Internal IP List (/usr/emerald/Emerald_BSM_EXPERT_Apr2000/resource-
object/config-TEST//local_netmap.conf)...load complete.
Access Policy Configuration File [/usr/emerald/Emerald_BSM_EXPERT_Apr2000/resource-
object/config-TEST//accesspolicy.conf] Loaded Successfully


INFORMATIVE (1): Disabling BSM_Make_Dot_File from knowledge-base


INFORMATIVE (1): Disabling BSM_Pepsi_Attack from knowledge-base


INFORMATIVE (1): Event Stream Source:  big_test.bsm.  (init)
```

```
---------------------------------------------------------------
ATTACK  (0|0|2)  BSM_PS_EXPLOIT   Target: 197.218.177.69   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 5584 LOCKOUT user_v
    Comment: root compromise

---------------------------------------------------------------
SEVERE WARNING  (1|1|6309) BSM_SELF_ECHO_ALERT Target: 130.107.12.102 Count: 6306
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 1999-04-05 17:17:10.0019PDT   End_time: 1999-04-05 17:18:09.9920PDT
    Command: echo   Parent_cmd: inetd   Outcome: 0
    Attacker: 172.16.114.50
    Recommendation: FILTER 172.16.114.50
    Comment: relevant params: BSM_MAX_ECHOS_RECEIVED, BSM_ECHO_FLOOD_WINDOW

---------------------------------------------------------------
ATTACK  (2|2|6562)  BSM_BUFFER_OVERFLOW_EXEC   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 24792 LOCKOUT admin_u
    Comment: root compromise

---------------------------------------------------------------
WARNING  (3|3|6575)  BSM_SUSPICIOUS_EXEC_ARGUMENT  Target: 130.107.15.118  Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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
    Comment: relevant params: BSM_SUSPICIOUS_EXEC_LIST

---------------------------------------------------------------
WARNING  (4|4|6576)  BSM_SUSPICIOUS_EXEC_ARGUMENT  Target: 130.107.15.118  Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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
    Comment: relevant params: BSM_SUSPICIOUS_EXEC_LIST
```

```
---------------------------------------------------------------
ATTACK  (5|5|6644)  BSM_SPECIAL_USER_EXEC   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 25039
    Comment: relevant params: BSM_EXEC_LESS_ACCOUNTS

---------------------------------------------------------------
ATTACK  (6|6|6652)  BSM_SPECIAL_USER_EXEC   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 25039
    Comment: relevant params: BSM_EXEC_LESS_ACCOUNTS

---------------------------------------------------------------
ATTACK  (7|7|6676)  BSM_EXEC_NON_AUTHOR   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 25336 ISOLATE /usr/emerald/em_user1/sample
    Comment: relevant params: BSM_LAST_RESERVED_ACCOUNT

---------------------------------------------------------------
WARNING  (8|8|6743)  BSM_ROOT_CORE_CREATE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /export/home/core

---------------------------------------------------------------
SEVERE WARNING  (9|9|6834)  BSM_ROOT_CORE_ACCESS Target: 130.107.15.118 Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /export/home/core

----------------------------------------------------------------
ATTACK  (10|10|7188)  BSM_CHANGE_USER_ENVIRON_FILE   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:12:56.712041 PST
    Command: creat(2)   Parent_cmd: /usr/bin/vi   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001 ruid = 50001 euid = 50001 pid = 25389 sid = 25336
    Resource: /usr/emerald/em_user2/.cshrc   Resource_owner: not_present
    Recommendation: ISOLATE /usr/emerald/em_user2/.cshrc
    Comment: relevant params: BSM_USER_ENV_FILES

----------------------------------------------------------------
ATTACK  (11|11|7203)  BSM_CHANGE_USER_ENVIRON_FILE   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:13:14.562088 PST
    Command: creat(2)   Parent_cmd: /usr/bin/touch   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001 ruid = 50001 euid = 50001  pid = 25391 sid = 2533
    Resource: /usr/emerald/em_user2/.rhosts   Resource_owner: em_user1
    Recommendation: ISOLATE /usr/emerald/em_user2/.rhosts
    Comment: relevant params: BSM_USER_ENV_FILES

----------------------------------------------------------------
ATTACK  (12|12|7204)  BSM_CHANGE_USER_ENVIRON_FILE   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:13:14.562088 PST
    Command: old utime(2)   Parent_cmd: /usr/bin/touch   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001 ruid = 50001 euid = 50001 pid = 25391 sid = 25336
    Resource: /usr/emerald/em_user2/.rhosts   Resource_owner: em_user1
    Recommendation: ISOLATE /usr/emerald/em_user2/.rhosts
    Comment: relevant params: BSM_USER_ENV_FILES

----------------------------------------------------------------
SEVERE WARNING  (13|13|7254)  BSM_ACCESS_PRIVATE_FILE   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /export/home/file1
    Comment: relevant params: BSM_USER_HOMES_LOCATION

----------------------------------------------------------------
WARNING  (14|14|7323)  BSM_SUSPICIOUS_SETUID   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /usr/emerald/em_user1/gurka
    Comment: relevant-params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
ATTACK  (15|15|7355)  BSM_SUSPICIOUS_SETUID   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 25336 ISOLATE /usr/emerald/em_user1/file_owned_by_2
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
SEVERE WARNING  (16|16|7401)  BSM_ROOT_CORE_EVENT Target: 130.107.15.118  Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /export/home/core

---------------------------------------------------------------
WARNING  (17|17|7506)  BSM_MAKE_TEMP_SYM   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 1999-12-30 16:17:15.672732 PST
    Command: symlink(2)   Parent_cmd: /usr/bin/ln   Outcome: 0
    Attacker: em_user1
    Attacker_attrs: auid = 50001 ruid = 50001 euid = 50001 pid = 25420 sid = 25336
    Resource: /tmp/grepa   Resource_owner: em_user1
    Recommendation: ISOLATE /tmp/grepa

---------------------------------------------------------------
ATTACK  (18|18|7528)  BSM_ILLEGAL_SHADOW_PASSWD_ACCESS   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 25336 LOCKOUT em_user1
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
ATTACK  (19|19|7553)  BSM_PROMISCUOUS_MODE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 25336 LOCKOUT em_user1
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST, BSM_EMERALD_NIC_NAMES

---------------------------------------------------------------
ATTACK  (20|20|7591)  BSM_MOD_SYSTEM_EXECUTABLE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 25039 LOCKOUT admin_u ISOLATE /usr/bin/who
    Comment: relevant params: BSM_SYSTEM_BIN_LOCATIONS

---------------------------------------------------------------
ATTACK  (21|21|7600)  BSM_MOD_SYSTEM_EXECUTABLE   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 25039 LOCKOUT admin_u ISOLATE /usr/bin/who
    Comment: relevant params: BSM_SYSTEM_BIN_LOCATIONS

---------------------------------------------------------------
SEVERE WARNING  (22|22|7620)  BSM_MOD_SYSTEM_RESOURCE   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /var/log/.nasty
    Comment: relevant params: BSM_SYSTEM_LOG_LOCATIONS, BSM_SYSTEM_RESOURCE_FILES,
                              BSM_LAST_RESERVED_ACCOUNT

---------------------------------------------------------------
WARNING  (23|23|7695)  BSM_SUSPICIOUS_SETUID   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /usr/emerald/em_user1/csh
    Comment: relevant-params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
WARNING  (24|24|7775)  BSM_SUSPICIOUS_SETUID   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /tmp/gurka
    Comment: relevant-params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
ATTACK  (25|25|7864)  BSM_ROOT_BY_NONADMIN   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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 25336 LOCKOUT em_user1
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
ATTACK  (26|26|7970)  BSM_ROOT_BY_NONADMIN   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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 25336 LOCKOUT em_user1
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
ATTACK  (27|27|8071)  BSM_ROOT_BY_NONADMIN   Target: 130.107.15.118   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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 25336 LOCKOUT em_user1
    Comment: relevant params: BSM_ADMINISTRATIVE_USER_LIST

---------------------------------------------------------------
WARNING  (28|28|8229)  BSM_REACH_MAX_BADLOGIN   Target: 130.107.15.118   Count: 4
    Observer: eXpert-BSM   Observer_Location: tuvok   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
    Comment: 130.107.15.118 login - telnet [ invalid user name ] from invalid uname
    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  (29|29|8569)  BSM_PROC_EXHAUST_THRESHOLD   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 15242
    Comment: relevant params: BSM_MAX_FAILED_PROCS_PER_CYCLE,
                              BSM_FAILED_PROCS_THRESHOLD_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (30|30|8723)  BSM_FILE_EXHAUST_THRESHOLD   Target: 130.107.15.118
Count: 8
    Observer: eXpert-BSM   Observer_Location: tuvok   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 /mnt/floppy/sample3
    Comment: relevant params: BSM_MAX_NOSPACE_ERRORS,
                              BSM_WRITE_ERR_THRESHOLD_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (31|31|8731)  BSM_FILE_EXHAUST_THRESHOLD   Target: 130.107.15.118
Count: 8
    Observer: eXpert-BSM   Observer_Location: tuvok   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 /mnt/floppy/sample3
    Comment: relevant params: BSM_MAX_NOSPACE_ERRORS,
                              BSM_WRITE_ERR_THRESHOLD_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (32|32|8766)  BSM_ATTEMPTED_ROOT_LOGIN   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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
    Comment: Attempted remote root login

---------------------------------------------------------------
SEVERE WARNING  (33|33|8768)  BSM_ATTEMPTED_ROOT_LOGIN   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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
    Comment: Attempted remote root login

---------------------------------------------------------------
WARNING  (34|34|9530)  BSM_SUSPICIOUS_PORT_PROBE   Target: 130.107.12.102  Count: 4
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 2000-01-14 08:12:34.3789PST   End_time: 2000-01-14 08:12:34.4689PST
    Command: connect   Parent_cmd: not_present   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: target_ports = [ 13 540 512 21 ]
    Comment: relevant params: BSM_PORTHIT_WARNING, BSM_PORT_ANALYSIS_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (35|35|9677)  BSM_SUSPICIOUS_PORT_PROBE   Target: 130.107.12.102
Count: 4
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 2000-01-14 08:16:33.0739PST   End_time: 2000-01-14 08:16:33.9939PST
    Command: connect   Parent_cmd: not_present   Outcome: 0
    Attacker: 130.107.15.118
    Attacker_attrs: target_ports = [ 25 513 23 21 ]
    Comment: relevant params: BSM_PORTHIT_WARNING, BSM_PORT_ANALYSIS_WINDOW

---------------------------------------------------------------
ATTACK  (36|36|9890)  BSM_SUSPICIOUS_PORT_PROBE   Target: 130.107.12.102   Count: 8
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 2000-01-14 08:21:49.2104PST  End_time: 2000-01-14 08:21:49.4004PST
    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 ]
    Comment: relevant params: BSM_PORTHIT_WARNING, BSM_PORT_ANALYSIS_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (37|37|10065)  BSM_BAD_PORT_CONNECTION   Target: tuvok   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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 130.107.15.118
    Comment: relevant params: BSM_UNACCEPTABLE_PORT_CONNECTIONS, host and net lists
in /usr/emerald/Emerald_BSM_EXPERT_Apr2000/resource-object/config-
TEST//local_netmap.conf

---------------------------------------------------------------
SEVERE WARNING  (38|38|10280)  BSM_FTP_USERNAME_GUESSER   Target: tuvok   Count: 7
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 09:41:57.0825PST  End_time: 2000-01-21 09:42:44.0215PST
    Command: open(2) - read,write   Parent_cmd: <unknown-122>   Outcome: 0
    Attacker: non_present
    Attacker_attrs: auid = 0  ruid = 0  euid = 0  pid = 122  sid = 0
    Recommendation: FILTER 130.107.12.103
    Comment: relevant params: BSM_MAX_FTP_BADPASSWORDS, BSM_FAILED_LOGIN_WINDOW

---------------------------------------------------------------
SEVERE WARNING  (39|39|10526)  BSM_FTP_PASSWD_GUESSER   Target: tuvok   Count: 6
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 09:47:23.046354 PST   End_time: 2000-01-21
09:51:39.851549 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
    Comment: relevant params: BSM_MAX_FTP_BADPASSWORDS, BSM_FAILED_LOGIN_WINDOW
```

```
--------------------------------------------------------------
ATTACK  (40|40|10599)  BSM_FTP_ANON_WRITE   Target: tuvok   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /usr/local/ftp/pub/upload/passwd FILTER 130.107.12.103
    Comment: relevant params: BSM_FTP_UPLOAD_PATHS, BSM_LOCAL_FTPD_UID,
                              BSM_ANON_FILE_EXPIRE

--------------------------------------------------------------
ATTACK  (41|41|10693)  BSM_FTP_ANON_WRITE   Target: tuvok   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: ISOLATE /usr/local/ftp/pub/warez/win2000 FILTER 130.107.12.103
    Comment: relevant params: BSM_FTP_UPLOAD_PATHS, BSM_LOCAL_FTPD_UID,
                              BSM_ANON_FILE_EXPIRE

--------------------------------------------------------------
WARNING  (42|42|10949)  BSM_FTP_WAREZ_ACTIVITY   Target: not_present   Count: 5
    Observer: eXpert-BSM   Observer_Location: tuvok   Observer_src:  big_test.bsm
    Start_time: 2000-01-21 09:54:08.1886PST  End_time: 2000-01-21 09:55:57.5061 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: ISOLATE /usr/local/ftp/pub/warez/win2000
    Comment: relevant params: BSM_FTP_WAREZ_COMPLAINT, BSM_LOCAL_FTPD_UID

--------------------------------------------------------------
WARNING  (43|43|11516)  BSM_DISALLOWED_FILE_EXEC  Target: 130.107.15.118  Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 2647 LOCKOUT em_user1
    Comment: see accesspolicy.conf

--------------------------------------------------------------
SEVERE WARNING  (44|44|11518)  BSM_DISALLOWED_FILE_EXEC  Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 2647 LOCKOUT em_user1
    Comment: see accesspolicy.conf

---------------------------------------------------------------
WARNING  (45|45|11538)  BSM_DISALLOWED_FILE_READ   Target: 130.107.15.118  Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 2647 LOCKOUT em_user1
    Comment: see accesspolicy.conf

---------------------------------------------------------------
SEVERE WARNING  (46|46|11553) BSM_DISALLOWED_FILE_READ  Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 2647 LOCKOUT em_user1
    Comment: see accesspolicy.conf

---------------------------------------------------------------
WARNING  (47|47|11794)  BSM_DISALLOWED_FILE_WRITE  Target: 130.107.15.118  Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 2647 LOCKOUT em_user1
    Comment: see accesspolicy.conf

---------------------------------------------------------------
SEVERE WARNING  (48|48|11840)  BSM_DISALLOWED_FILE_WRITE   Target: 130.107.15.118
Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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: KILL 2647 LOCKOUT em_user1 ISOLATE /accounting/DBMS/payroll.db
    Comment: see accesspolicy.conf

---------------------------------------------------------------
WARNING  (49|49|11919)  BSM_DISALLOWED_FILE_READ   Target: tuvok   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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 2822 LOCKOUT em_user1 FILTER 130.107.15.118
    Comment: see accesspolicy.conf.  relevant params: BSM_LOCAL_FTPD_UID

----------------------------------------------------------------
SEVERE WARNING  (50|50|11920)  BSM_DISALLOWED_FILE_READ   Target: tuvok   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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 2822 LOCKUOUT em_user1 FILTER 130.107.15.118
    Comment: see accesspolicy.conf.  relevant params: BSM_LOCAL_FTPD_UID

----------------------------------------------------------------
SEVERE WARNING  (51|51|12070)  BSM_TIME_WARP   Target: 130.107.12.102   Count: 1
    Observer: eXpert-BSM   Observer_Location: tuvok   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 ntp
    Comment: relevant params: BSM_MAX_BACKWARD_TIME

appcommon.c:208 NoDataCB(SignificantEvent):

Interface close (idle 2000 msec) event-manager saw 12072 events, last seq # 12071,
max idle 360000 msec


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