The MITRE Corporation

Results Interpretation within the Common Operating Environment Kernel Platform Certification Security Test Plan's Automated Environment

February 11, 2002

Prepared by:

James A. Finegan
The MITRE Corporation
Center for Integrated Intelligence Systems
7515 Colshire Drive
McLean, VA 22102-7508

Executive Summary

This document provides interpretation recommendations to Common Operating Environment (COE) Kernel Platform Certification (KPC) test engineers on automated test steps within the Security Test Plan (STP) that may require formal administrative resolution.

Documented herein is a summary of tests that have been tagged as failures by the Host-Oriented Security Test Suite (HOSTS) utility. Many of these failures result from conditions that cannot be predicted in advance. Consequently, the results from the step require human review to interpret the validity of the failure.

Chapter

1

Introduction

Purpose and Background

This document provides explanations for several test steps that may fail under the Common Operating Environment (COE) Kernel Platform Certification (KPC) prototype configuration. These failures are the result of security testing using Host-Oriented Security Test Suite (HOSTS) technology. Since HOSTS technology reduces the pass/fail criteria into a simple true or false condition, tests that cannot always be reduced to such succinct terms may produce false negatives. Consequently, these steps may require administrative interpretation before a determination can be made on whether or not the failure truly represents a security test failure. All test step failures documented herein fall into the following three categories:

1. True failures that result from changes having been made to the system.
   a. Residuals from other testing efforts that have changed the configuration.
   b. Changes made for convenience.
2. Operational errors
   a. Failures in a sequence of critical steps that resulted when a specific resource had been granted to another process during the middle of the critical test sequence process.
   b. Failure to properly prepare for test sequence execution.
   c. Failure to respond properly for required input.
3. Hardware and/or software configuration differences.
   a. Drivers.
   b. Installed software.
   c. Kernel release.

Several of the KPC failures were encountered while testing the Solaris 8 prototype system are listed in this document. Others are test steps where the potential for failure is self-evident (e.g., the list of known privileged binaries on a given system).

Scope and Approach

The approach detailed in this document is to present a table for each of the test steps that may require administrative resolution. Each table will include a sample HOSTS-generated failure message, a description of what action the test step is performing and a guide on interpreting the result.

This is NOT a definitive list for all failures. Consequently, under other environments such as COE security testing, there may be additional failures encountered that represent detection of improper settings and/or behavior.

Document Organization

This document contains three remaining sections: Terminology and Issues, Administrative Resolution Results, and Recommendations.

Chapter

2

Terminology and Issues

What Does Administrative Resolution Mean?

Definition:

Administrative Resolution is defined as the act of a competent individual evaluating what appears to be a failed test to determine both cause and applicability. In some circumstances, the failed result may be reclassified.

How does the administrative resolution work?

If the automated test process fails a given step, the lead test engineer will need to evaluate whether or not the test step truly represents a security failure. This is done through evaluation of the failed step against the guidance criteria presented in this document.

What Are the Issues?

Why is there a need for Administrative Resolution?

One of the goals for the task under which the HOSTS utility was developed was to develop a tool that could eliminate the need for human interpretation of results. Every effort was made to achieve this goal.

As development continued, it became apparent that it would not be possible to construct several key tests that compare the candidate's environment against an expected environment in such a way that a failure was unambiguous. It was found that many of these tests were impacted by both the hardware configuration for the candidate under tests as well as the software installed on that candidate. While the basic configuration was set, the variations introduced by the candidates hardware configuration could not be predicted.

Other tests that examine object reuse within the UNIX kernel were impacted by system activity. While these steps passed approximately

80% of the time, the 20% failure rate was indicative of the need for external review before either a PASS or NOT TESTABLE resolution can be declared.

Finally, the automated process uncovered several residuals associated with the manual test process. Since these residuals do affect the performance of the automated tool as well as the security posture of the candidate system, a discussion on identifying and correcting these particular steps failed was needed.

Chapter
3

Administrative Resolution Results

The investigation results herein apply to systems built in accordance with the *Defense Information Infrastructure (DII) Common Operating Environment (COE) Setup Procedures for Kernel Platform Certification (KPC) Validation Cell for Kernel V4.2.0.6 (Solaris 8)*.

Version Series Tests

No `version_series` test steps are known to fail KPC testing on the prototype system. It should be noted that the entire test process has been configured to abort if an attempt is made to utilize the automated test utility on operating systems other than the one for which it was configured. In this particular case, the operating system is Solaris 8.

Identification and Authentication Series Tests

The following `ia_series` test steps have been known to periodically fail KPC testing on the prototype system.

Test Steps: IA-1.B.12 and IA-1.B.14

```
Test: IA-1.B.12                  Test Description:
===========================================================================
CUSP:                            Verify no guest accounts detected in
Req. Spec.: I4.2.2.4P1           password file

  Test Command(s):
  -------------------------------------------------------------------------
  test_parameter_count "^(guest|visit|temp|tmp|generic|other)" 0
  /etc/passwd

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  --------------------------  ---------------------------------------------
  match            no match   Pattern encountered = 2


Test: IA-1.B.14                  Test Description:
===========================================================================
CUSP:                            Verify no guest accounts detected in
Req. Spec.: I4.2.2.4P1           shadow file

  Test Command(s):
  -------------------------------------------------------------------------
```

Test Steps: IA-1.B.12 and IA-1.B.14

```
test_parameter_count "^(guest|visit|temp|tmp|generic|other)" 0
/etc/shadow

<------------------------------- Results ------------------------------->
Expected           Actual   Data Returned:
-------------------------   ---------------------------------------------
match            no match   Pattern encountered = 2
```

These steps fail when at least one account was found on the system that begin with one of the following strings:

guest   visit   temp   tmp   generic   other

These strings represent common account naming formats for what are collectively known as "guest" accounts. Since, the Security Requirements Specification (SRS) for COE does not permit guest accounts, they should be removed:

```
userdel <temp account name>
```

FAILURE   This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Steps: IA-2.D.29 and IA-2.F.4.2

```
Test: IA-2.D.29                  Test Description:
===========================================================================
CUSP:                            Verify minimum password age limit has been
Req. Spec.: 3.2.1.4.1.1.4.1,     defined to one week
            3.2.1.4.1.2

  Test Command(s):
  -------------------------------------------------------------------------
  test_parameter "^MINWEEKS=1" /etc/default/passwd

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  found           not found


Test: IA-2.F.4.2                 Test Description:
===========================================================================
CUSP:                            Verify minimum password age limit has been
Req. Spec.: 3.2.1.4.1.1.4.1      defined to one week

  Test Command(s):
  -------------------------------------------------------------------------
  test_parameter "^MINWEEKS=1" /etc/default/passwd

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  found           not found
```

These steps fail because the minimum password age value has been set to a value other than the COE required minimum (one week). The minimum password age limit needs to be reset in `/etc/default/passwd` to the following:

```
MINWEEKS=1
```

Test Steps: IA-2.D.29 and IA-2.F.4.2

FAILURE	This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Steps: IA-2.G.3.5 and IA-2.G.3.7

```
Test: IA-2.G.3.5                 Test Description:
==========================================================================
CUSP:                            Verify privileged user is able to change
Req. Spec.: 3.2.1.4.1.4,         password on another account
            3.2.1.6.5,
            3.2.16.2.4

  Test Command(s):
  ------------------------------------------------------------------------
  run_command '/usr/bin/passwd IAaccnt1'

  <------------------------------ Results ------------------------------>
  Expected           Actual   Data Returned:
  -------------------------   --------------------------------------------
  match          unexpected   Non-zero exit status of 1 returned.


Test: IA-2.G.3.7                 Test Description:
==========================================================================
CUSP:                            Verify user account is no longer locked
Req. Spec.: 3.2.1.4.1.4,
            3.2.1.6.5,
            3.2.16.2.4

  Test Command(s):
  ------------------------------------------------------------------------
  test_parameter_count "PS" 1 /tmp/IA-2.IAaccnt1

  <------------------------------ Results ------------------------------>
  Expected           Actual   Data Returned:
  -------------------------   --------------------------------------------
  match            no match   Pattern encountered = 0
```

This test will fail if a valid password is not entered at the following prompt:

```
OPERATOR ACTION:
----
Please enter a password, press return, enter the password
again and press return a second time. Nothing will be
displayed on the screen.
```

UNRESOLVED	The appropriate action is to re-run the test series entering the password correctly as directed.

Audit Series Tests

The following `audit_series` test steps have been known to periodically fail KPC testing on the prototype system.

Test Step: ADT-3.G.30.5

Test Step: ADT-3.G.30.5

```
Test: ADT-3.G.30.5               Test Description:
===================================================================
CUSP:                            Rename the not-terminated file to reduce
Req. Spec.:                      future confusion

  Test Command(s):
  -----------------------------------------------------------------
  run_command "/bin/mv /security1/*not_terminated* /security1/ADT-
  3.terminated_abruptly"

  <------------------------------ Results ------------------------------>
  Expected          Actual   Data Returned:
  -------------------------  --------------------------------------------
  match         unexpected   Non-zero exit status of 2 returned.
```

This step typically fails when more than one audit trail files exist in `/security1` with names that contain the string "`not_terminated`". Since only the most recent file is active, the mere presence of additional such files is an indication that the audit daemon had been shut down improperly at some point.

Test series procedure calls for the clean up of the `/security1` directory prior to execution of the `audit_series` tests. This is emphasized when the following comment is displayed during set-up:

```
Now Processing: Test Setup
             ----
                Did audit data directory get cleaned up BEFORE running
                this test?
```

UNRESOLVED — The appropriate action is to re-run the test series after cleaning both `/security1` and `/security2` as directed.

Test Step: ADT-2.E.5.1

```
Test: ADT-2.E.5.1                Test Description:
===================================================================
CUSP:                            Verify /etc/security is sufficiently
Req. Spec.: 3.2.3.1.2,           protected
            3.2.3.1.2.2

  Test Command(s):
  -----------------------------------------------------------------
  test_protection_minimum drwxr-x--- /etc/security

  <------------------------------ Results ------------------------------>
  Expected          Actual   Data Returned:
  -------------------------  --------------------------------------------
  match           no match   Candidate(s) did not match minimum
                             protection.
```

This step fails because of changes that have been made to the system after the installation of the basic COE kernel. Systems tested with only the kernel installed (e.g., no optional segments) will pass this test.

The recommended fix is to add ADT-2.E.6.1 to `SKIPTEST` until the cause for this anomaly can be identified and corrected.

UNRESOLVED — The appropriate action is to re-run the test series after the

Test Step: ADT-2.E.5.1

above-described change has been made to the test series.

Test Steps: ADT-4.H.99.2a and ADT-4.H.99.2b

```
Test: ADT-4.H.99.2a              Test Description:
 ===========================================================================
 CUSP:                            Verify date and time is stored in each
 Req. Spec.: 3.2.3.5.1            audit record

   Test Command(s):
   -------------------------------------------------------------------------
   test_parameter_count "(Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)
   [0123][0-9] [012][0-9]:[0-6][0-9]:[0-6][0-9] 20[0-9][0-9]" 1
   /tmp/Audit_log

   <------------------------------- Results ------------------------------->
   Expected           Actual   Data Returned:
   -------------------------   ---------------------------------------------
   match            no match   Pattern encountered = 0


 Test: ADT-4.H.99.2b              Test Description:
 ===========================================================================
 CUSP:                            Verify date and time is stored in each
 Req. Spec.: 3.2.3.5.1            audit record

   Test Command(s):
   -------------------------------------------------------------------------
   test_parameter_count "[0123][0-9] (Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|
   Oct|Nov|Dec) 20[0-9][0-9] [012][0-9]:[0-6][0-9]:[0-6][0-9]" 1
   /tmp/Audit_log

   <------------------------------- Results ------------------------------->
   Expected           Actual   Data Returned:
   -------------------------   ---------------------------------------------
   match            no match   Pattern encountered = 0
```

Steps ADT-4.H.99.2a and ADT-4.H.99.2b are mutually exclusive. In other words, only one of these two test steps can pass in the environment under test. Which one will pass is dependent upon both the default shell used for the test and how the system level date control variables are defined.

If ADT-4.H.99.2a fails, the recommended fix is to add ADT-4.H.99.2a to SKIPTEST and remove ADT-4.H.99.2b from SKIPTEST. If ADT-4.H.99.2b fails, the recommended fix is to add ADT-4.H.99.2b to SKIPTEST and remove ADT-4.H.99.2a from SKIPTEST.

UNRESOLVED	The appropriate action is to re-run the test series after the above-described change has been made to the test series.

Miscellaneous Series Tests

The following misc_series test steps have been known to periodically fail KPC testing on the prototype system.

Test Step: MISC-3.C.3.9

```
Test: MISC-3.C.3.9               Test Description:
===========================================================================
CUSP:                            Verify ftpd network protocol is disabled
Req. Spec.: 3.2.1.5,             by default
            3.2.1.5.1,
            3.2.2.1,
            I4.2.2.5.9

  Test Command(s):
  -------------------------------------------------------------------------
  test_parameter '^ftp' /etc/inet/inetd.conf

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  not found           found   ftp stream tcp6 nowait root
                              /opt/tcpd/bin/tcpd in.ftpd -dl -t60
```

This test step failed because the system has the FTP daemon enabled within `/etc/initd.conf`. By default, the COE installation procedure disables this daemon. Consequently, this daemon had to have been enabled after the system was installed. It is often enabled to facilitate transferring files and not disabled afterwards.

The fix is to disable FTP daemon in `/etc/inetd.conf`.

FAILURE	This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Steps: MISC-5.E.1.10 and MISC-5.E.1.23

```
Test: MISC-5.E.1.10              Test Description:
===========================================================================
CUSP:                            Verify test file inodes were actually the
Req. Spec.: 3.2.10.1             same showing inode reuse had occurred

  Test Command(s):
  -------------------------------------------------------------------------
  files_differ "/tmp/root_MISC-5-initial" "/tmp/root_MISC-5-recreate

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match            no match   Candidate file(s) did not match.  1c1   <
                              236737476 /tmp/root_MISC-5   ---   >
                              235068651 /tmp/root_MISC-5


Test: MISC-5.E.1.23              Test Description:
===========================================================================
CUSP:                            Verify test file inodes were actually the
Req. Spec.: 3.2.10.1             same showing inode reuse had occurred

  Test Command(s):
  -------------------------------------------------------------------------
  files_differ "/tmp/root_MISC-5-initial" "/tmp/root_MISC-5-recreate

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match            no match   Candidate file(s) did not match.  1c1   <
                              236737476 /tmp/root_MISC-5   ---   >
```

Test Steps: MISC-5.E.1.10 and MISC-5.E.1.23

```
235068651 /tmp/root_MISC-5
```

This step will fail from time to time, particularly on a system where there is any other activity besides the testing. It is used to provide a “level of comfort” in the C2 certification by demonstrating data stored at a particular location on a disk is not made available to the next user of that location.

This test sequence performs the following:

1. Create a file
2. Put data in the file
3. Capture the inode for the file (e.g., starting block number on the disk on which the file was created)
4. Delete the file
5. Create a new file
6. Compare the inode of the new file with that of the old file. If they are the same, the same physical starting point on the disk has been used for the new file. (If the inodes do not match, some other process came in and grabbed the newly freed block. This can happen on active systems - as we see from this failure.)
7. Read the contents of the newly created file. If they match what was put into the file in step 2, we have clear "Object Re-use" which means the C2 requirement for object re-use is not being met. (This is the requirements verification step.)

This step, which corresponds to item 6 above, will simply fail from time to time. Experience has shown that the failure rate is less than 20% on a relatively calm system.

PASS	One or more of the following test steps DID NOT fail: MISC-5.E.1.10, MISC-5.E.1.23, and OS-271.GG.1.18. These all are doing the same thing. Consequently, if at lease one of these passed (e.g., does not show up on the list of failed tests), this failure can be ignored.
UNRESOLVED	If all three test steps failed, and the test has not been re-run more than once, the appropriate action is to re-run the test series when the system is quiet.
NOT_TESTABLE	If this test has been re-run three or more times without any of the three test steps (MISC-5.E.1.10, MISC-5.E.1.23, and OS-271.GG.1.18) passing, these steps are to be classified as not testable.

Operating System Tests

The following `os_series` test steps have been known to periodically fail KPC testing on the prototype system.

Test Step: OS-57.F.3.3

```
Test: OS-57.F.3.3                Test Description:
===========================================================================
CUSP:                            Verify root account home directory is
Req. Spec.: 3.2.15.1,            properly group protected
            3.2.15.2, 3.2.5.3,
            3.2.5.6

  Test Command(s):
  -------------------------------------------------------------------------
  test_group "root|other" /

  <------------------------------ Results ------------------------------>
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match            no match   Candidate file(s) did not match expected
                              group.  Found: staff  Expected: root|other
```

The group ownership of the root partition (/) has changed. Under the typical Solaris installation, the group ownership will be `root.` This value has been found to change when an improperly constructed tarball is installed.

The group identifier should be reset to its default value:

```
cd /; chgrp root /
```

FAILURE	This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Step: OS-57.F.3a

```
Test: OS-57.F.3a                 Test Description:
===========================================================================
CUSP:                            Verify root home directory is owned and
Req. Spec.: 3.2.15.1,            protected properly - method 2
            3.2.15.2, 3.2.5.6

  Test Command(s):
  -------------------------------------------------------------------------
  test_home_dir_files drwxr-xr-x 'root' '.'

  <------------------------------ Results ------------------------------>
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match           not found   None of the file names specified were found
                              in the user home directories.
```

The group ownership of the root partition (/) has changed. Under the typical Solaris installation, the group ownership will be `root.` This value has been found to change when an improperly constructed tarball is installed.

The group identifier should be reset to its default value:

```
cd /; chgrp root /
```

Test Step: OS-57.F.3a

FAILURE	This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Step: OS-57.F.7.4

```
Test: OS-57.F.7.4                Test Description:
===========================================================================
CUSP:                            Verify all user startup files are owned
Req. Spec.: 3.2.15.1,            and protected properly
            3.2.15.2, 3.2.5.6

  Test Command(s):
  -------------------------------------------------------------------------
  test_home_dir_files -rwxr-xr-x 'ALL' '.[a-zA-Z]*'

  <------------------------------ Results ------------------------------>
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match             partial   The following valid users matched ownership
                      match   and protection requirements:  user1 user2
                              user3 user4 user5 user6 secman sysadmin  The
                              following valid users did not match ownership
                              and protection requirements:  user7
                              Invalid/bypassed user accounts: root daemon
                              bin sys adm lp uucp nobody noaccess listen
                              nuucp nobody4 COE SA SSO
```

One or more user accounts on an active system were found to have the looser than SRS required protection settings (e.g., a umask of 027) on files and/or directories within their home directory.

The user should issue the following command to reset protections:

```
cd; chmod -R o-rwx . ; chmod –R g-w .
```

FAILURE	This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Steps: OS-60.G.3.1 and OS-60.G.3.2

```
Test: OS-60.G.3.1                Test Description:
===========================================================================
CUSP:                            Verify tape device is sufficiently
Req. Spec.: 3.2.5.11,            protected
            3.2.5.11.1,
            3.2.5.6

  Test Command(s):
  -------------------------------------------------------------------------
  test_protection_minimum -rw-rw---- '/dev/rmt/*'

  <------------------------------ Results ------------------------------>
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match|not        no match   Candidate(s) did not match minimum
  found                       protection.


Test: OS-60.G.3.2                Test Description:
===========================================================================
CUSP:                            Verify compatibility tape devices are
```

Test Steps: OS-60.G.3.1 and OS-60.G.3.2

```
Req. Spec.: 3.2.5.11,           sufficiently protected
            3.2.5.11.1,
            3.2.5.6

  Test Command(s):
  -------------------------------------------------------------------------
  test_protection_minimum -rw-rw---- '/dev/rst* /dev/nrst*'

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match|not        no match   Candidate(s) did not match minimum
  found                       protection.
```

This test will fail on systems where tape devices have been added to the system without removing world access to the tape device. The test essentially uses an "ls -ld" command, comparing the results with the expected results.

The recommended temporary fix would be to add test steps OS-60.G.3.1 and OS-60.G.3.1 to the `SKIPTEST` list within the `os_series` file.

UNRESOLVED	The appropriate action is to re-run the test series after the above-described change has been made to the test series.

Test Step: OS-88.L.3.5

```
Test: OS-88.L.3.5                Test Description:
===========================================================================
CUSP:                            Verify the R daemons are not enabled in
Req. Spec.: 3.2.1.1,             /etc/inetd.conf
            3.2.1.1.1,
            3.2.1.1.2,
            3.2.2.2, 3.2.5.6,
            3.2.15.3,
            I4.2.1.2.3

  Test Command(s):
  -------------------------------------------------------------------------
  test_parameter "^(shell|login|exec)" /etc/inetd.conf

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  not found           found   login stream tcp6 nowait root
                              /usr/sbin/in.rlogind in.rlogind
```

This test step failed because the system has the Berkeley "rlogin" daemon enabled within `/etc/initd.conf`. By default, the COE installation procedure disables this daemon. Consequently, this daemon had to have been enabled after the system was installed. It is typically a residual from other sections of the testing process. The fix is to disable the Berkeley “R” command daemons in `/etc/inetd.conf`.

FAILURE	This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Step: OS-98.P.9.3

```
Test: OS-98.P.9.3                Test Description:
===========================================================================
```

Test Step: OS-98.P.9.3

```
    CUSP:                            Verify there are no accounts that have not
    Req. Spec.: 3.2.1.5,             been active within this month or last
                3.2.16.5.3           month

      Test Command(s):
      -----------------------------------------------------------------------
      test_dormant_accounts

      <------------------------------ Results ------------------------------>
      Expected           Actual   Data Returned:
      -------------------------   -------------------------------------------
      CLEAN             WARNING   The following inactive accounts were found:
                                  secman keyman
```

This step will fail if the listed accounts had not been logged into prior to the first execution of STPAUT. Since the password-setting vehicle logs one off the system immediately after setting a new password, each account should be manually logged into as verification that the password was properly reset.

The recommended fix is to set passwords for the three base accounts (secman, keyman and sysadmin) PRIOR to actually beginning the test run. Other inactive accounts should be disabled using:

```
passwd –l <idle account>
```

UNRESOLVED   The appropriate action is to re-run the test series after the above-described action has been taken.

Test Step: OS-121.T.4.18

```
    Test: OS-121.T.4.18              Test Description:
    =========================================================================
    CUSP:                            Verify other group access is limited
    Req. Spec.: 3.2.5.3, 3.2.5.6,
                3.2.15.3

      Test Command(s):
      -----------------------------------------------------------------------
      test_status "/bin/awk -F: '(\$3 == 1) {print \$4}' /etc/group" ""

      <------------------------------ Results ------------------------------>
      Expected           Actual   Data Returned:
      -------------------------   -------------------------------------------
      match            no match   Expected and returned values did not match
                                  Expected = , Returned = solusr01
```

This step will fail if a user account is found to belong to a group with a GID value less than 20. The recommended fix is to remove the unauthorized user account from the privileged group. This can be done by editing `/etc/group`.

FAILURE   This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Steps: OS-260.FF.3.13 and OS-260.FF.3.14

```
    Test: OS-260.FF.3.13             Test Description:
    =========================================================================
    CUSP:                            Verify tape device is sufficiently
```

Test Steps: OS-260.FF.3.13 and OS-260.FF.3.14

```
    Req. Spec.: 3.2.5.11,            protected
                3.2.5.11.1,
                3.2.5.6, 3.2.15.3

      Test Command(s):
      -------------------------------------------------------------------------
      test_protection_minimum -rw-rw---- '/dev/rmt/*'

      <------------------------------- Results ------------------------------->
      Expected           Actual   Data Returned:
      -------------------------   ---------------------------------------------
      match|not        no match   Candidate(s) did not match minimum
      found                       protection.

    Test: OS-260.FF.3.14             Test Description:
    ===========================================================================
    CUSP:                            Verify compatibility tape devices are
    Req. Spec.: 3.2.5.11,            sufficiently protected
                3.2.5.11.1,
                3.2.5.6, 3.2.15.3

      Test Command(s):
      -------------------------------------------------------------------------
      test_protection_minimum -rw-rw---- '/dev/rst* /dev/nrst*'

      <------------------------------- Results ------------------------------->
      Expected           Actual   Data Returned:
      -------------------------   ---------------------------------------------
      match|not        no match   Candidate(s) did not match minimum
      found                       protection.
```

This test will fail on systems where tape devices have been added to the system without removing world access to the tape device. The test essentially uses an "ls -ld" command, comparing the results with the expected results.

The recommended temporary fix would be to add test steps OS-260.FF.3.13 and OS-260.FF.3.14 to the `SKIPTEST` list within the `os_series` file.

UNRESOLVED	The appropriate action is to re-run the test series after the above-described change has been made to the test series.

Test Step: OS-271.GG.1.18

```
    Test: OS-271.GG.1.18             Test Description:
    ===========================================================================
    CUSP:                            Verify test file inodes were actually the
    Req. Spec.: 3.2.10.1             same showing inode reuse had occurred

      Test Command(s):
      -------------------------------------------------------------------------
      files_differ "/tmp/root_OS-271-initial" "/tmp/root_OS-271-recreate"

      <------------------------------- Results ------------------------------->
      Expected           Actual   Data Returned:
      -------------------------   ---------------------------------------------
      match            no match   Candidate file(s) did not match.  1c1   <
                                  236737476 /tmp/root_OS-271   ---   >
                                  235068651 /tmp/root_OS-271
```

This step will fail from time to time, particularly on a system where there is any other activity besides the testing. It is used to provide a “level of comfort” in the C2 certification by demonstrating data stored at a particular location on a disk is not

Test Step: OS-271.GG.1.18

made available to the next user of that location.

This test sequence performs the following:

1. Create a file
2. Put data in the file
3. Capture the inode for the file (e.g., starting block number on the disk on which the file was created)
4. Delete the file
5. Create a new file
6. Compare the inode of the new file with that of the old file. If they are the same, the same physical starting point on the disk has been used for the new file. (If the inodes do not match, some other process came in and grabbed the newly freed block. This can happen on active systems - as we see from this failure.)
7. Read the contents of the newly created file. If they match what was put into the file in step 2, we have clear "Object Re-use" which means the C2 requirement for object re-use is not being met. (This is the requirements verification step.)

This step, which corresponds to item 6 above, will simply fail from time to time. Experience has shown that the failure rate is less than 20% on a relatively calm system.

PASS	One or more of the following test steps DID NOT fail: MISC-5.E.1.10, MISC-5.E.1.23, and OS-271.GG.1.18. These all are doing the same thing. Consequently, if at lease one of these passed (e.g., does not show up on the list of failed tests), this failure can be ignored.
UNRESOLVED	If all three test steps failed, and the test has not been re-run more than once, the appropriate action is to re-run the test series when the system is quiet.
NOT_TESTABLE	If this test has been re-run three or more times without any of the three test steps (MISC-5.E.1.10, MISC-5.E.1.23, and OS-271.GG.1.18) passing, these steps are to be classified as not testable.

Test Step: OS-271.GG.1.36

```
Test: OS-271.GG.1.36              Test Description:
======================================================================
CUSP:                             Verify only strangely named files are
Req. Spec.:                       expected from either end-user or full OS
                                  installation

  Test Command(s):
  --------------------------------------------------------------------
  multi_part_test 'tests/plugins/files_differ_field 8 "/tmp/OS-271-suspect-
  filtered" "baseline/known-strange-name-files-full"' 'match'
  'tests/plugins/files_differ_field 8 "/tmp/OS-271-suspect-filtered"
```

Test Step: OS-271.GG.1.36

```
"baseline/known-strange-name-files-end-user"' 'match'

<------------------------------ Results ------------------------------>
Expected           Actual   Data Returned:
-------------------------   ------------------------------------------
match|no         no match   One or more of the expected and returned
match                both   values did not match    Expected =  1:match
one|no                      2:match    Returned =    1:no match
match two                   Candidate file(s) did not match.   More data
                            is in /tmp/OS-271-suspect-filtered than in
                            baseline/known-strange-name-files-full
                            2:no match   Candidate file(s) did not match.
                            More data is in baseline/known-strange-name-
                            files-end-user than in /tmp/OS-271-suspect-
                            filtered
```

See the following two files:

```
/tmp/OS-271-suspect-filtered
/h/data/local/STPAUT/<os>/baseline/known-strange-name-files-end-user
```

After filtering, there are: 1) more files with unusual names than expected, or, 2) fewer files with unusual names than expected. Compare the listed files line by line until the differences are found. The test engineer will need to determine if the differences are related to a segment or other software product that has been installed in the local environment. Common examples of segments that could add files with unusual names scripts include the COE kernel itself. This step is expected to fail when running the test series developed for a kernel specific release on a kernel of a different release.

To reset the baseline to match the current local configuration, the test engineer can replace the baseline configuration file using:

```
cp /tmp/OS-271-suspect-filtered \
 /h/data/local/STPAUT/<os>/baseline/known-strange-name-files-end-user
```

Be sure to edit `/h/data/local/STPAUT/<os>/baseline/known-strange-name-files-end-user` afterwards to insure only expected files and directories are listed.

PASS	All of the differences can be attributed to recent known changes to the system (e.g., installation or removal of software). In addition, all files are owned by a privileged account such as root or COE.
FAIL	1) The existence of one or more files in `/tmp/OS-271-suspect-filtered` and not in `known-strange-name-files-end-user` cannot be explained through recent system activity, such as software installation. 2) One or more files in `/tmp/OS-271-suspect-filtered` is owned by a non-privileged account.

Discretionary Access Control Tests

The following `dac_series` test steps have been known to periodically fail testing on the KPC prototype system.

Test Step: DAC-4.D.19.2

```
Test: DAC-4.D.19.2                Test Description:
===========================================================================
CUSP:                             Verify root home directory is owned and
Req. Spec.: 3.2.5.6, 3.2.15.3,    protected properly
            3.2.16.1,
            I4.2.2.3.1P2

  Test Command(s):
  -------------------------------------------------------------------------
  test_home_dir_files drwxr-xr-x 'root' '.'

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match           not found   None of the file names specified were found
                              in the user home directories.
```

The group ownership of the root partition (/) has changed. Under the typical Solaris installation, the group ownership will be `root.` This value has been found to change when an improperly constructed tarball is installed.

The group identifier should be reset to its default value:

```
cd /; chgrp root /
```

FAILURE This is a common residual and/or convenience problem. Consequently, it represents a FAILURE condition.

Test Step: DAC-4.D.87.4

```
Test: DAC-4.D.87.4                Test Description:
===========================================================================
CUSP:                             Verify no unexpected world writable
Req. Spec.: 3.2.5.6, 3.2.15.1,    directories exist without the sticky bit
            3.2.15.3,             set
            I4.2.2.7P1

  Test Command(s):
  -------------------------------------------------------------------------
  files_differ_field 8 "/tmp/DAC-4-world-dir-ns"
  "baseline/known-non-sb-ww-directories"

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match            no match   Candidate file(s) did not match.  More data
                              is in baseline/known-non-sb-ww-directories
                              than in /tmp/DAC-4-world-dir-ns
```

See the following two files:

```
    /tmp/DAC-4-world-dir-ns
```

Test Step: DAC-4.D.87.4

```
    /h/data/local/STPAUT/<os>/baseline/known-non-sb-ww-directories
```

After filtering, there are: 1) more world-write enabled directories than expected, or, 2) fewer world-write enabled directories than expected. Compare the listed files line by line until the differences are found. The test engineer will need to determine if the differences are related to a segment or another software product that has been installed in the local environment. Common examples of segments that could add additional world-write enabled include GCCS. This step is expected to fail when running the test series developed for a kernel specific release on a kernel of a different release.

To reset the baseline to match the current local configuration, the test engineer can replace the baseline configuration file using:

```
 cp /tmp/DAC-4-world-dir-ns \
  /h/data/local/STPAUT/<os>/baseline/known-non-sb-ww-directories
```

Be sure to edit `/h/data/local/STPAUT/<os>/baseline/known-non-sb-ww-directories` afterwards to insure only expected directories are listed.

PASS	All of the differences can be attributed to recent known changes to the system (e.g., installation or removal of software). In addition, all directories are owned by a privileged account such as root or COE and have the “sticky” bit set.
FAIL	1) The existence of one or more directories in `/tmp/DAC-4-world-dir-ns` and not in `known-non-sb-ww-directories` cannot be explained through recent system activity, such as software installation. 2) One or more directories in `/tmp/DAC-4-world-dir-ns` is owned by a non-privileged account. 3) One or more directories in `/tmp/DAC-4-world-dir-ns` does not have the “sticky” bit set.

Test Step: DAC-4.D.88.3

```
Test: DAC-4.D.88.3               Test Description:
===========================================================================
CUSP:                            Verify only known binary SetUID and SetGID
Req. Spec.: 3.2.5.6, 3.2.15.1,   files listed in known-setuid-setgid-files
            3.2.15.3,            were detected under either end-user or
            I4.3.1.5, I4.3.2.2   full OS installation modes

  Test Command(s):
  -------------------------------------------------------------------------
  multi_part_test 'tests/plugins/files_differ_field 8 "/tmp/DAC-4-priv"
  "baseline/known-setuid-setgid-files-full"' 'match'
  'tests/plugins/files_differ_field 8 "/tmp/DAC-4-priv" "baseline/known-
  setuid-setgid-files-end-user"' 'match'

  <------------------------------- Results ------------------------------->
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match|no         no match   One or more of the expected and returned
```

Test Step: DAC-4.D.88.3

```
      match               both   values did not match    Expected =  1:match
      one|no                     2:match    Returned =    1:no match
      match two                  Candidate file(s) did not match.   More data
                                 is in baseline/known-setuid-setgid-files-full
                                 than in /tmp/DAC-4-priv    2:no match
                                 Candidate file(s) did not match.   More data
                                 is in /tmp/DAC-4-priv than in baseline/known-
                                 SETUID-SETGID-FILES-END-USER
```

See the following two files:

```
   /tmp/DAC-4-priv
   /h/data/local/STPAUT/<os>/baseline/known-setuid-setgid-files-end-user
```

After filtering, there are: 1) more binaries with enhanced privileges than expected, or, 2) fewer binaries with enhanced privileges than expected. Compare the listed files line by line until the differences are found. The test engineer will need to determine if the differences are related to a segment, another software product, or hardware that has been installed in the local environment. Common examples of segments that could add additional binaries include GCCS. This step is expected to fail when running the test series developed for a kernel specific release on a kernel of a different release.

To reset the baseline to match the current local configuration, the test engineer can replace the baseline configuration file using:

```
 cp /tmp/DAC-4-priv \
  /h/data/local/STPAUT/<os>/baseline/known-setuid-setgid-files-end-user
```

Be sure to edit `/h/data/local/STPAUT/<os>/baseline/known-setuid-setgid-files-end-user` afterwards to insure only expected binary files are listed. (For example, HP-UX does not alter the privileges of archived binary files that are "replaced" when security patches are installed.)

PASS	All of the differences can be attributed to recent known changes to the system (e.g., installation or removal of software or hardware) and/or hardware drivers unique to the system. In addition, all files are owned by a privileged account such as root or COE.
FAIL	1) The existence of one or more files in `/tmp/DAC-4-priv` and not in known`-setuid-setgid-files-end-user` cannot be explained through recent system activity, such as software or hardware installation. 2) One or more files in `/tmp/DAC-4-priv` is owned by a non-privileged account.

Test Step: DAC-4.D.88.5

```
    Test: DAC-4.D.88.5               Test Description:
    ===========================================================================
    CUSP:                            Verify only known non-binary SetUID and
    Req. Spec.: 3.2.5.6, 3.2.15.1,   SetGID files listed in known-non-binary-
```

Test Step: DAC-4.D.88.5

```
            3.2.15.3,           setuid were detected
            I4.3.1.5, I4.3.2.2

    Test Command(s):
    ------------------------------------------------------------------------
    multi_part_test 'tests/plugins/files_differ_field 8 "/tmp/DAC-4-non-bin"
    "baseline/known-non-binary-setuid-full"' 'match' 'tests/plugins/
    files_differ_field 8 "/tmp/DAC-4-non-bin" "baseline/known-non-binary-
    setuid-end-user end-user"' 'match'

    <------------------------------- Results ------------------------------->
    Expected          Actual   Data Returned:
    -------------------------  ---------------------------------------------
    match|no         no match  One or more of the expected and returned
    match                both  values did not match    Expected =  1:match
    one|no                     2:match    Returned =    1:no match
    match two                  Candidate file(s) did not match.   More data
                               is in /tmp/DAC-4-non-bin than in
                               baseline/known-non-binary-setuid-full    2:no
                               match  Candidate file(s) did not match.
                               More data is in /tmp/DAC-4-non-bin than in
                               baseline/known-non-binary-setuid-end-user
```

See the following two files:

```
   /tmp/DAC-4-non-bin
   /h/data/local/STPAUT/<os>/baseline/known-non-binary-setuid-end-user
```

After filtering, there are: 1) more shell scripts with enhanced privileges than expected, or, 2) fewer shell scripts with enhanced privileges than expected. Compare the listed files line by line until the differences are found. The test engineer will need to determine if the differences are related to a segment or other software product that has been installed in the local environment. Common examples of segments that could add additional privileged scripts include GCCS. This step is expected to fail when running the test series developed for a kernel specific release on a kernel of a different release.

To reset the baseline to match the current local configuration, the test engineer can replace the baseline configuration file using:

```
 cp /tmp/DAC-4-non-bin \
  /h/data/local/STPAUT/<os>/baseline/known-non-binary-setuid-end-user
```

Be sure to edit `/h/data/local/STPAUT/<os>/baseline/known-non-binary-setuid-end-user` afterwards to insure only expected non-binary files are listed.

PASS	All of the differences can be attributed to recent known changes to the system (e.g., installation or removal of software). In addition, all files are owned by a privileged account such as root or COE.
FAIL	1) The existence of one or more files in `/tmp/DAC-4-non-bin` and not in `known-non-binary-setuid-end-user` cannot be explained through recent system activity, such as software installation.

Test Step: DAC-4.D.88.5

	2) One or more files in /tmp/DAC-4-non-bin is owned by a non-privileged account.

Test Step: DAC-4.D.89.4

```
Test: DAC-4.D.89.4              Test Description:
===========================================================================
CUSP:                           Verify only c-shell files listed in known-
Req. Spec.: 3.2.5.6, 3.2.15.1,  c-shells are detected under either end-
            3.2.15.3,           user or full OS installation modes
            I4.3.1.5, I4.3.2.2

  Test Command(s):
  -------------------------------------------------------------------------
  multi_part_test 'tests/plugins/files_differ_field 8 "/tmp/DAC-4-c-shell"
  "baseline/known-c-shells-full"' 'match' 'tests/plugins/files_differ_field
  8 "/tmp/DAC-4-c-shell" "baseline/known-c-shells-end-user"' 'match'

  <------------------------------ Results ------------------------------>
  Expected           Actual   Data Returned:
  -------------------------   ---------------------------------------------
  match|no         no match   One or more of the expected and returned
  match                both   values did not match    Expected =  1:match
  one|no                      2:match    Returned =    1:no match
  match two                   Candidate file(s) did not match.   More data
                              is in /tmp/DAC-4-c-shell than in
                              baseline/known-c-shells-full    2:no match
                              Candidate file(s) did not match.   More data
                              is in /tmp/DAC-4-c-shell than in
                              baseline/known-c-shells-end-user
```

See the following two files:

```
/tmp/DAC-4-c-shell
/h/data/local/STPAUT/<os>/baseline/known-c-shells-end-user
```

There are: 1) more C-shell scripts than expected, or, 2) fewer C-shell scripts than expected. Compare the listed files line by line until the differences are found. The test engineer will need to determine if the differences are related to a segment or other software product that has been installed in the local environment. Common examples of segments that could add additional C-shell scripts include GCCS. This step is expected to fail when running the test series developed for a kernel specific release on a kernel of a different release.

To reset the baseline to match the current local configuration, the test engineer can replace the baseline configuration file using:

```
cp /tmp/DAC-4-c-shell \
 /h/data/local/STPAUT/<os>/baseline/known-c-shells-end-user
```

Be sure to edit /h/data/local/STPAUT/<os>/baseline/known-c-shells-end-user afterwards to insure only expected C-Shell files are listed.

PASS	All of the differences can be attributed to recent known changes to the system (e.g., installation or removal of software). In addition, all files

<table>
<tr><th colspan="2">Test Step: DAC-4.D.89.4</th></tr>
<tr><td></td><td>are owned by a privileged account such as root or COE.</td></tr>
<tr><td>FAIL</td><td>1) The existence of one or more files in <code>/tmp/DAC-4-c-shell</code> and not in <code>known-c-shells-end-user</code> cannot be explained through recent system activity, such as software installation or user account creation.
2) One or more files in <code>/tmp/DAC-4-c-shell</code> and not in <code>known-c-shells-end-user</code> is owned by a non-privileged account. In addition, the listed C-Shell scripts do not represent the standard C-Shell login scripts (e.g., .cshrc and .login)</td></tr>
</table>

Chapter

4

Recommendations

This section is not applicable in the context of this document.

Appendix

Problem Reporting, Waivers and Interpretations[1]

Information about the procedures for applying for interpretations and waivers can be found on The Open Group's World Wide Web site, at the URL:

http://www.opengroup.org/interpretations

A searchable database of existing interpretations and waivers is available at the URL

http://www.opengroup.org/interpretations/database

.

[1] This page was appended to the original Mitre document