Hardening VMS Nodes

1 Introduction

If a customer requests that their system meet the SCADA security level for compliance with the Department of defense (DoD) Security Technical Implementation Guide (STIG), a list of requirements can be obtained from the latest revision of the general purpose operating system Security Requirements Guide (SRG), which can be downloaded from:
https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=operating-systems%2Cgeneral-purpose-os
since there is no OpenVMS-specific set of requirements created by the DoD.

This document describes the way to mitigate some of the issues causing noncompliance between the STIG-provided requirements and a real system. Considering the STIG contents, all items on its list may belong to one of the following groups:

1. "Not a finding" items. These are the system features, which are in compliance with the SRG specifications.
2. "Not applicable" items. The features that do not exist in the product and therefore cannot be exploited, belong here.
3. "Finding" items. The features that do not match the SRG-outlined requirements. This group can represent several types of incompatibilities:
    a. Fixable features, which can be reconfigured to match the requirements.
    b. Unfixable features, which cannot be modified due to operating system limitations.
    c. Critical features, which cannot be changed, so as to not comprise system availability (the functionality the system serves for).

This document describes the procedure to be used to mitigate the "fixable features" and to improve the user's experience when using the security-related features.

2 Areas of Application

Reconfigured by this package, OpenVMS options are intended to:

- Provide for the system break-in information auditing.
- Provide for the login failure auditing.
- Provide for the login success auditing.
- Provide for the logout auditing.
- Provide for the authorization database access / changes auditing.
- Provide for the network configuration auditing.
- Provide for the INSTALL utility use auditing.
- Provide for the privileged activities (failures and success) auditing.
- Provide for the object creation and deletion auditing.

- Implement DoD-required login banners.
- Adjust the user's login settings.
- Provide for the required passwords security level.
- Secure the login procedure.

3 Hardening Package

This package is part of the MISER distribution code. It is located in `[MISER.SOURCE.SYS$SERVICE.HARDENING]` and consists of the following files (new and modified compared to the regular MISER contents). These files comprise several groups used for:

1. System hardening installation (runs once):
   - `NODE_HARDENING.COM`
   - `MOD$ACCOUNTS_SECURITY.COM`
   - `MOD$CONFIGURE_GENERIC.COM`
   - `MOD$SITE_CMDS.COM`
   - `MOD$SYLOGIN.COM`
   - `MOD$SYSGEN_PARAMS.COM`
   - `MOD$TOOL_CMDS.COM`
   - ENABLE$AUDIT.COM
2. Hardening runtime support (modifies system behavior as needed):
   - `PWD_CHECKER.COM`
   - `UAL_ADDUSER.COM`
   - `UAL_DISTRIBUTER.COM`
   - `UAL_MODUSER.COM`
   - `WARNING_JPEG.JPG`
   - `WARNING_TEXT.TXT`
   - `AUDIT_SCHEDULE.COM`
   - `AUDIT_QUEUETEST.COM`
3. Backup (preserves original system files):
   - `UAL_ADDUSER.COM_TEMPLATE`
   - `UAL_DISTRIBUTER.COM_TEMPLATE`
   - `UAL_MODUSER.COM_TEMPLATE`
4. Service (simplifies the user experience):
   - `AUDIT_PEEK.COM`
   - `LOGON.COM`

All files should be copied to a user-selected directory. For example, to: `[USERS.SYSTEM.HARDENING]` (the user must have **SYSPRV** privileges in order to run this procedure). The command to start it is:

```
$ @node_hardening
```

The procedure should be executed on each OpenVMS node independently.

The procedure prints out the list of the modified system files and the list of modified user accounts. The following system files can also be changed by this procedure:

- SITE$COM:SITE_COMMANDS.COM
- MNET$COM:START_MISER.COM
- SYS$STARTUP:SYLOGIN.COM

After the procedure is completed (it takes about a dozen seconds or longer depending on the number of registered user accounts) it is recommended that you make arrangements to the sys$startup:sylogin.com files, which may exist in different directories. Actually, sys$startup is a system logical that corresponds to three physical locations.

- SYS$SYSROOT:[SYS$STARTUP]
- SYS$SYSROOT:[SYSMGR]
- SYS$COMMON:[SYSMGR]

Each of these directories can (and often do) contain some versions of sylogin.com file. In order to make the situation manageable, it is a best practice to:

- Rename all the previously used file entries.
- Remove all unused file entries.

So that only one syslogin.com file would be available.

The result may look like:

```
USRVSA$ dir sys$startup:sylogin*.com /dat /siz

Directory SYS$SYSROOT:[SYSMGR]

Directory SYS$SYSROOT:[SYSMGR]
SYLOGIN.COM;2                    19    NOVEMBER 3, 2020 04:41 PM
SYLOGIN_PREV.COM;1               18    JANUARY 3, 2007 02:07 PM
Total of 2 files, 37 blocks.

Directory SYS$COMMON:[SYSMGR]
SYLOGIN_OLD.COM;1                13    OCTOBER 2, 2001 01:47 PM
Total of 1 file, 13 blocks.

Grand total of 2 directories, 3 files, 50 blocks.
```

After the installation, the system should be rebooted.

4 Changes to the System

There are two sorts of changes applied by the hardening procedure to the operating system: hidden and visible. The hidden are (according to their name) not immediately observable by the end-users (like adding certain information to the audit file). The visible changes are noticeable and therefore should be known and understood.

The login banners are changed according to the DoD rules. There are two banners: text-oriented and graphics-oriented login. Both of them display the same text:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

• The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

• At any time, the USG may inspect and seize data stored on this IS.

• Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

• This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

• Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

In the text-oriented login cases though, unlike the graphics-oriented ones, the operating system requests the user's confirmation and proceeds only if the user agrees with the banner's contents.

- The number of the failed login attempts that can occur before the system takes action against a possible break-in, is set to 100.
- The length of the failure monitoring period is set to five seconds.
- The default file protection is set to (RWED, RWED,RE,).
- The minimum password length is set to sixteen characters.
- The password is case-sensitive and includes an extended special characters set (all keyboard characters except the double quote (").
- The password policy requires that any password must include at least one each of the following:
  - A lowercase character
  - An uppercase character
  - A digit
  - A special character

NOTE 1: The package makes it possible for a customer to tweak the password requirements changing them according to their "local" requirements. In order to change the above defaults you must redefine the global symbol **PWD_COMPLEXITY**.

The structure of this symbol's value is:
[L[U[D[S]]]][,[M][,E]

Where the brackets denote all elements being optional:

- **L** — this digit represents the minimum number of lowercase characters in the password.
- **U** — this digit denotes the minimum number of uppercase characters.
- **D** — this digit defines the minimum number of digits.
- **S** — this digit denotes the minimum number of special characters.
- **M** — this number limits the minimum password length.
- **E** — this number defines the number of days before the password expires and should be changed.

Parameters **M** and **E** should be delimited with commas. However, the trailing comma(s) can be omitted.

If any of the above parameters are not defined, the default value is used. The default symbol value is:
1111,16,60

NOTE 2: In order to enforce this policy you should use the MISER **UAL** procedure only, not the native OpenVMS **AUTHORIZE** utility.

The password lifetime is set to sixty days (i.e., the password must be changed at least every sixty days, while the system memorizes and rejects the previously used passwords).

NOTE 3: The password related changes (length, lifetime, and case-sensitivity) are only applicable for the end-user's accounts, not for altering "system", "hsq", and "ucx" accounts.

NOTE 4: After applying the described changes, users' passwords will become case-sensitive, which is different from the default setup (where they are not and could be provided in any case). According to the OpenVMS internals, the case-sensitive passwords are saved as uppercase; therefore, the affected users will have to type their old password in all uppercase.

The audit journal file: SYS$COMMON:[SYSMGR]SECURITY.AUDIT$JOURNAL is recreated automatically once per quarter in order to keep it manageable.

5 Introduced Service Options

5.1 Helper Audit Records Viewer

Since the system hardening assumes a significant increase in audit information, reviewing this information may be confusing. In order to assist an end-user retrieving information, there is a command file called: `Mnet$com:peek_audit.com`, which guides an operator through the request setup making the process logical and simple.

The procedure is not intended to replace the system's ANALYZE utility, it offers a small (but important) subset of options related to the audit journal review.

To start the viewer, you should use the command:

```
$ @Mnet$com:audit_peek
```

The procedure will then show the following menu:

```
============================================================
This utility allows displaying information about most common
events collected by the system inside the audit database

What events are you interested in and what would like to do?
A - Changes to the authorization database (SYSUAF.DAT,
    RIGHTSLIST.DAT, NETPROXY.DAT, or NET$PROXY.DAT)
B - Break-in detection
F - Unsuccessful login attempts
I - Successful logins
O - Successful logouts
G - Modification of system parameters through the
    System Generation utility (SYSGEN) or AUTOGEN
N - Modification of the DECnet network configuration
U - Modification of the system user authorization file
* - All events
M - Display this menu
E - Exit
Make your selection [E]:
```

A user can select the topic of interest (audit records to review) by typing a corresponding letter and pressing <Enter>. After which the procedure will prompt the user to specify the date interval to be reviewed. The prompt looks like below:

```
Now you can define the date interval to search for
the above-selected events. You will be prompted for
the start and end dates, which can be specified as:
  1. dd-mmm-yyyy - which denotes day-month-year, or
  2. today       - or
  3. yesterday   - or
  4. tomorrow    - which would mean including todays records, or
  5. all         - which eliminates the search limit, or
  6. boot        - which denotes the date when the
                   system was most recently started.
The default for the start date is yesterday, and for
the end date is tomorrow, that is by default the
report will show the information collected during
two last days.
Specify the selection start date [yesterday]:
```

As soon as the user specifies the start date, they are prompted to specify the ending date as well:

```
Specify the selection end date [now]:
```

At this point the procedure starts looking into the audit database, picking up the related records and displaying them one-by-one in the screen (if there anything to show). The user can either look at the records by pressing <Enter> after each record by pressing <Ctrl>+<C>. In either case, the user will be switched back to the main menu for a new mode selection.

5.2 SSH Login Helper

The SSH login option provides for securely logging in (unlike the regular DECnet-based login) and at the same time allows logging in to the physically remote nodes, while DECnet can only be used at limited distances. However, these commands are non-uniform and negatively effects the user experience.

In order to make the SSH login user-friendly, the `Mnet$com:logon.com` command file was created and the system-level "LOGIN" symbol has been added to the symbols table. Login can be initiated by typing either:

```
$ login <nodename>
```

Or:

```
$ login
```

The <nodename> represents the DECnet name of the destination node or its IP address. If the <nodename> parameter is not specified (the second form of the command above), the user is prompted to specify it. If the user skips the <nodename> value (i.e., presses <Enter> in response to the nodename prompt), then self-login is assumed (i.e., logging in to the source node itself).

As soon as the nodename is provided, the user is prompted to provide the username for the account to log in to. If the username is omitted, the procedure quits. Otherwise, it requests the password for the specified user's account.