1.4 Configure Bootloader

The recommendations in this section focus on securing the bootloader and settings involved in the boot process directly.

1.4.1 Ensure bootloader password is set (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters

Rationale:

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off AppArmor at boot time).

Impact:

If password protection is enabled, only the designated superuser can edit a GRUB 2 menu item by pressing "e" or access the GRUB 2 command line by pressing "c"

If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable to do so, the configuration files will have to be edited via a LiveCD or other means to fix the problem

You can add `--unrestricted` to the menu entries to allow the system to boot without entering a password. A password will still be required to edit menu items.

More Information: https://help.ubuntu.com/community/Grub2/Passwords

Audit:

Run the following commands and verify output matches:

```
# grep "^set superusers" /boot/grub/grub.cfg

set superusers="<username>"
# awk -F. '/^\s*password/ {print $1"."$2"."$3}' /boot/grub/grub.cfg

password_pbkdf2 <username> grub.pbkdf2.sha512
```

Remediation:

Create an encrypted password with `grub-mkpasswd-pbkdf2`:

```
# grub-mkpasswd-pbkdf2 --iteration-count=600000 --salt=64

Enter password: <password>
Reenter password: <password>
PBKDF2 hash of your password is <encrypted-password>
```

Add the following into a custom `/etc/grub.d` configuration file:

```
cat <<EOF
exec tail -n +2 $0
set superusers="<username>"
password_pbkdf2 <username> <encrypted-password>
EOF
```

The superuser/user information and password should not be contained in the `/etc/grub.d/00_header` file as this file could be overwritten in a package update.
If there is a requirement to be able to boot/reboot without entering the password, edit `/etc/grub.d/10_linux` and add `--unrestricted` to the line `CLASS=`
Example:

```
CLASS="--class gnu-linux --class gnu --class os --unrestricted"
```

Run the following command to update the `grub2` configuration:

```
# update-grub
```

Default Value:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub/grub.cfg` with the appropriate grub configuration file for your environment.

References:

1. NIST SP 800-53 Rev. 5: AC-3

Additional Information:

Changes to `/etc/grub.d/10_linux` may be overwritten during updates to the `grub-common` package. You should review any changes to this file before rebooting otherwise the system may unexpectedly prompt for a password on the next boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1542, T1542.000	TA0003	M1046

1.4.2 Ensure access to bootloader config is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The grub configuration file contains information on boot settings and passwords for unlocking boot options.

Rationale:

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `0600` or more restrictive.

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)'
/boot/grub/grub.cfg

Access: (0600/-rw-------)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set permissions on your grub configuration:

```
# chown root:root /boot/grub/grub.cfg
# chmod u-x,go-rwx /boot/grub/grub.cfg
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3

Additional Information:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub/grub.cfg` with the appropriate grub configuration file for your environment

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1542, T1542.000	TA0005, TA0007	M1022

1.5 Configure Additional Process Hardening

1.5.1 Ensure address space layout randomization is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

Rationale:

Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.randomize_va_space` is set to `2`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   a_output=(); a_output2=(); a_parlist=(kernel.randomize_va_space=2)
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   f_kernel_parameter_chk()
   {
      l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
      if grep -Pq -- '\b'"$l_parameter_value"'\b' <<<
"$l_running_parameter_value"; then
         a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\""
         "    in the running configuration")
      else
         a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"" \
         "    in the running configuration" \
         "    and should have a value of: \"$l_value_out\"")
      fi
      unset A_out; declare -A A_out # Check durable setting (files)
      while read -r l_out; do
         if [ -n "$l_out" ]; then
            if [[ $l_out =~ ^\s*# ]]; then
               l_file="${l_out//# /}"
            else
               l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
               [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_file")
            fi
         fi
      done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([^#\n\r]+|#\h*\/[^#\n\r\h]+\.conf\b)')
      if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
         l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
         l_kpar="${l_kpar//\//.}"
         [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_ufwscf")
      fi
      if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
         while IFS="=" read -r l_fkpname l_file_parameter_value; do
            l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
            if grep -Pq -- '\b'"$l_parameter_value"'\b' <<<
"$l_file_parameter_value"; then
               a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"" \
               "    in \"$(printf '%s' "${A_out[@]}")\"")
            else
               a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\""
               "    in \"$(printf '%s' "${A_out[@]}")\"" \
               "    and should have a value of: \"$l_value_out\"")
            fi
         done < <(grep -Po -- "^\h*$l_parameter_name\h*=\h*\H+" 
"${A_out[@]}")
      else
         a_output2+=(" - \"$l_parameter_name\" is not set in an included 
file" \
         "    ** Note: \"$l_parameter_name\" May be set in a file that's 
ignored by load procedure **")
      fi
   }
   l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
   while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and 
check parameters
      l_parameter_name="${l_parameter_name// /}"; 
l_parameter_value="${l_parameter_value// /}"
      l_value_out="${l_parameter_value//-/ through }"; 
l_value_out="${l_value_out//|/ or }"
      l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
      f_kernel_parameter_chk
   done < <(printf '%s\n' "${a_parlist[@]}")
   if [ "${#a_output2[@]}" -le 0 ]; then
      printf '%s\n' "" "- Audit Result:" "  ** PASS **" "${a_output[@]}" ""
   else
      printf '%s\n' "" "- Audit Result:" "  ** FAIL **" " - Reason(s) for 
audit failure:" "${a_output2[@]}"
      [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:" 
"${a_output[@]}" ""
   fi
}
```

Remediation:

Set the following parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending in .conf:

- kernel.randomize_va_space = 2

Example:

```
# printf "%s\n" "kernel.randomize_va_space = 2" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.randomize_va_space=2
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

kernel.randomize_va_space = 2

References:

1. http://manpages.ubuntu.com/manpages/focal/man5/sysctl.d.5.html
2. CCI-000366: The organization implements the security configuration settings
3. NIST SP 800-53 Rev. 5: CM-6

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000	TA0002	M1050

1.5.2 Ensure ptrace_scope is restricted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `ptrace()` system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers.

The sysctl settings (writable only with CAP_SYS_PTRACE) are:

- `0` - classic ptrace permissions: a process can PTRACE_ATTACH to any other process running under the same uid, as long as it is dumpable (i.e. did not transition uids, start privileged, or have called prctl(PR_SET_DUMPABLE...) already). Similarly, PTRACE_TRACEME is unchanged.
- `1` - restricted ptrace: a process must have a predefined relationship with the inferior it wants to call PTRACE_ATTACH on. By default, this relationship is that of only its descendants when the above classic criteria is also met. To change the relationship, an inferior can call prctl(PR_SET_PTRACER, debugger, ...) to declare an allowed debugger PID to call PTRACE_ATTACH on the inferior. Using PTRACE_TRACEME is unchanged.
- `2` - admin-only attach: only processes with CAP_SYS_PTRACE may use ptrace with PTRACE_ATTACH, or through children calling PTRACE_TRACEME.
- `3` - no attach: no processes may use ptrace with PTRACE_ATTACH nor via PTRACE_TRACEME. Once set, this sysctl value cannot be changed.

Rationale:

If one application is compromised, it would be possible for an attacker to attach to other running processes (e.g. Bash, Firefox, SSH sessions, GPG agent, etc) to extract additional credentials and continue to expand the scope of their attack.

Enabling restricted mode will limit the ability of a compromised process to PTRACE_ATTACH on other processes running under the same user. With restricted mode, ptrace will continue to work with root user.

Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.yama.ptrace_scope` is set to a value of: `1`, `2`, or `3`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   a_output=(); a_output2=(); a_parlist=("kernel.yama.ptrace_scope=(1|2|3)")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   f_kernel_parameter_chk()
   {
      l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
      if grep -Pq -- '\b'"$l_parameter_value"'\b' <<<
"$l_running_parameter_value"; then
         a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\""
         "    in the running configuration")
      else
         a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"" \
         "    in the running configuration" \
         "    and should have a value of: \"$l_value_out\"")
      fi
      unset A_out; declare -A A_out # Check durable setting (files)
      while read -r l_out; do
         if [ -n "$l_out" ]; then
            if [[ $l_out =~ ^\s*# ]]; then
               l_file="${l_out//# /}"
            else
               l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
               [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_file")
            fi
         fi
      done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([^#\n\r]+|#\h*\/[^#\n\r\h]+\.conf\b)')
      if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
         l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
         l_kpar="${l_kpar//\//.}"
         [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_ufwscf")
      fi
      if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
         while IFS="=" read -r l_fkpname l_file_parameter_value; do
            l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
            if grep -Pq -- '\b'"$l_parameter_value"'\b' <<<
"$l_file_parameter_value"; then
               a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"" \
               "    in \"$(printf '%s' "${A_out[@]}")\"")
            else
               a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\""
               "    in \"$(printf '%s' "${A_out[@]}")\"" \
               "    and should have a value of: \"$l_value_out\"")
            fi
         done < <(grep -Po -- "^\h*$l_parameter_name\h*=\h*\H+" 
"${A_out[@]}")
      else
         a_output2+=(" - \"$l_parameter_name\" is not set in an included 
file" \
         "    ** Note: \"$l_parameter_name\" May be set in a file that's 
ignored by load procedure **")
      fi
   }
   l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
   while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and 
check parameters
      l_parameter_name="${l_parameter_name// /}"; 
l_parameter_value="${l_parameter_value// /}"
      l_value_out="${l_parameter_value//-/ through }"; 
l_value_out="${l_value_out//|/ or }"
      l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
      f_kernel_parameter_chk
   done < <(printf '%s\n' "${a_parlist[@]}")
   if [ "${#a_output2[@]}" -le 0 ]; then
      printf '%s\n' "" "- Audit Result:" "  ** PASS **" "${a_output[@]}" ""
   else
      printf '%s\n' "" "- Audit Result:" "  ** FAIL **" " - Reason(s) for 
audit failure:" "${a_output2[@]}"
      [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:" 
"${a_output[@]}" ""
   fi
}
```

Remediation:

Set the `kernel.yama.ptrace_scope` parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf` to a value of `1`, `2`, or `3`:

```
kernel.yama.ptrace_scope = 1
    - OR -
kernel.yama.ptrace_scope = 2
    - OR -
kernel.yama.ptrace_scope = 3
```

Example:

```
# printf "%s\n" "kernel.yama.ptrace_scope = 1" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.yama.ptrace_scope=1
```

Note:

- If a value of `2` or `3` is preferred, or required by local site policy, replace the `1` with the desired value of `2` or `3` in the example above
- If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Default Value:

kernel.yama.ptrace_scope = 0

References:

1. https://www.kernel.org/doc/Documentation/security/Yama.txt
2. https://github.com/raj3shp/termspy
3. NIST SP 800-53 Rev. 5: CM-6

Additional Information:

Ptrace is very rarely used by regular applications and is mostly used by debuggers such as `gdb` and `strace`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1055, T1055.008	TA0005	M1040

1.5.3 Ensure core dumps are restricted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.

Rationale:

Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see `limits.conf(5)`). In addition, setting the `fs.suid_dumpable` variable to 0 will prevent setuid programs from dumping core.

Audit:

Run the following command and verify output matches:

```
# grep -Ps -- '^\h*\*\h+hard\h+core\h+0\b' /etc/security/limits.conf
/etc/security/limits.d/*

* hard core 0
```

Run the following script to verify `fs.suid_dumpable = 0`:
Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `fs.suid_dumpable` is set to `0`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   a_output=(); a_output2=(); a_parlist=("fs.suid_dumpable=0")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   f_kernel_parameter_chk()
   {
      l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
      if grep -Pq -- '\b'"$l_parameter_value"'\b' <<<
"$l_running_parameter_value"; then
         a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\""
         "    in the running configuration")
      else
         a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"" \
         "    in the running configuration" \
         "    and should have a value of: \"$l_value_out\"")
      fi
      unset A_out; declare -A A_out # Check durable setting (files)
      while read -r l_out; do
         if [ -n "$l_out" ]; then
            if [[ $l_out =~ ^\s*# ]]; then
               l_file="${l_out//# /}"
            else
               l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
               [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_file")
            fi
         fi
      done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([^#\n\r]+|#\h*\/[^#\n\r\h]+\.conf\b)')
      if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
         l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
         l_kpar="${l_kpar//\//.}"
         [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_ufwscf")
      fi
      if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
         while IFS="=" read -r l_fkpname l_file_parameter_value; do
            l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
            if grep -Pq -- '\b'"$l_parameter_value"'\b' <<<
"$l_file_parameter_value"; then
               a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"" \
               "    in \"$(printf '%s' "${A_out[@]}")\"")
            else
               a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\""
               "    in \"$(printf '%s' "${A_out[@]}")\"" \
               "    and should have a value of: \"$l_value_out\"")
            fi
         done < <(grep -Po -- "^\h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
      else
         a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
         "    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **")
      fi
   }
   l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
   while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
      l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
      l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
      l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
      f_kernel_parameter_chk
   done < <(printf '%s\n' "${a_parlist[@]}")
   if [ "${#a_output2[@]}" -le 0 ]; then
      printf '%s\n' "" "- Audit Result:" "  ** PASS **" "${a_output[@]}" ""
   else
      printf '%s\n' "" "- Audit Result:" "  ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
      [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
   fi
}
```

Run the following command to check if systemd-coredump is installed:

```
# systemctl list-unit-files | grep coredump
```

if anything is returned systemd-coredump is installed

Remediation:

Add the following line to `/etc/security/limits.conf` or a `/etc/security/limits.d/*` file:

```
* hard core 0
```

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `fs.suid_dumpable = 0`

Example:

```
# printf "\n%s" "fs.suid_dumpable = 0" >> /etc/sysctl.d/60-fs_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.suid_dumpable=0
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten
-IF- systemd-coredump is installed:
edit `/etc/systemd/coredump.conf` and add/modify the following lines:

```
Storage=none
ProcessSizeMax=0
```

Run the command:

```
systemctl daemon-reload
```

References:

1. NIST SP 800-53 Rev. 5: CM-6

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0007	M1057

1.5.4 Ensure prelink is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`prelink` is a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.

Rationale:

The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as libc.

Audit:

Verify `prelink` is not installed:

```
# dpkg-query -s prelink &>/dev/null && echo "prelink is installed"
```

Nothing should be returned.

Remediation:

Run the following command to restore binaries to normal:

```
# prelink -ua
```

Uninstall `prelink` using the appropriate package manager or manual installation:

```
# apt purge prelink
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1055, T1055.009, T1065, T1065.001	TA0002	M1050

1.5.5 Ensure Automatic Error Reporting is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Apport Error Reporting Service automatically generates crash reports for debugging

Rationale:

Apport collects potentially sensitive data, such as core dumps, stack traces, and log files. They can contain passwords, credit card numbers, serial numbers, and other private material.

Audit:

Run the following command to verify that the Apport Error Reporting Service is not enabled:

```
#  dpkg-query -s apport &> /dev/null && grep -Psi --
'^\h*enabled\h*=\h*[^0]\b' /etc/default/apport
```

Nothing should be returned
Run the following command to verify that the apport service is not active:

```
# systemctl is-active apport.service | grep '^active'
```

Nothing should be returned

Remediation:

Edit `/etc/default/apport` and add or edit the enabled parameter to equal `0`:

```
enabled=0
```

Run the following commands to stop and mask the apport service

```
# systemctl stop apport.service
# systemctl mask apport.service
```

- OR -
Run the following command to remove the apport package:

```
# apt purge apport
```

Default Value:

enabled=1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.6 Configure Command Line Warning Banners

Presenting a warning message prior to the normal user login may assist in the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.

Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at http://www.justice.gov/criminal/cybercrime/

The `/etc/motd`, `/etc/issue`, and `/etc/issue.net` files govern warning banners for standard command line logins for both local and remote users.

Note: The text provided in the remediation actions for these items is intended as an example only. Please edit to include the specific text for your organization as approved by your legal department.

1.6.1 Ensure message of the day is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/motd
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -
f2 | sed -e 's/"//g'))" /etc/motd
```

Remediation:

Edit the `/etc/motd` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`
- OR -
- IF - the `motd` is not used, this file can be removed.
Run the following command to remove the `motd` file:

```
# rm /etc/motd
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1082, T1082.000, T1592, T1592.004	TA0007	

1.6.2 Ensure local login warning banner is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version - or the operating system's name

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -
f2 | sed -e 's/"//g'))" /etc/issue
```

Remediation:

Edit the `/etc/issue` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`
Example:

```
# echo "Authorized users only. All activity may be monitored and reported." >
/etc/issue
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1082, T1082.000, T1592, T1592.004	TA0007	

1.6.3 Ensure remote login warning banner is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue.net
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -
f2 | sed -e 's/"//g'))" /etc/issue.net
```

Remediation:

Edit the `/etc/issue.net` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`
Example:

```
# echo "Authorized users only. All activity may be monitored and reported." >
/etc/issue.net
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	**Tactics**	**Mitigations**
T1018, T1018.000, T1082, T1082.000, T1592, T1592.004	TA0007	

1.6.4 Ensure access to /etc/motd is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Rationale:

- IF - the `/etc/motd` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify that if `/etc/motd` exists, `Access` is `644` or more restrictive, `Uid` and `Gid` are both `0/root`:

```
# [ -e /etc/motd ] && stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/
%G)' /etc/motd

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
  -- OR --
Nothing is returned
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/motd`:

```
# chown root:root $(readlink -e /etc/motd)
# chmod u-x,go-wx $(readlink -e /etc/motd)
```

- OR -
Run the following command to remove the `/etc/motd` file:

```
# rm /etc/motd
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

1.6.5 Ensure access to /etc/issue is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Rationale:

- IF - the `/etc/issue` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Access` is `644` or more restrictive and `Uid` and `Gid` are both `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/ %G)' /etc/issue

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: { 0/ root)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/issue`:

```
# chown root:root $(readlink -e /etc/issue)
# chmod u-x,go-wx $(readlink -e /etc/issue)
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

1.6.6 Ensure access to /etc/issue.net is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Rationale:

- IF - the `/etc/issue.net` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Access` is `644` or more restrictive and `Uid` and `Gid` are both `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/ %G)' /etc/issue.net

Access: (0644/-rw-r--r--)  Uid: ( 0/ root)   Gid: ( 0/ root)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/issue.net`:

```
# chown root:root $(readlink -e /etc/issue.net)
# chmod u-x,go-wx $(readlink -e /etc/issue.net)
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

1.7 Configure GNOME Display Manager

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

This subsection requires user profiles to already exist on the system. A profile is a list of configuration databases.

Sample profile:

```
user-db:user
system-db:local
system-db:site
```

Configuring a single user and multiple system databases allows for layering of preferences. Settings from the user database file take precedence over the settings in the local database file, and the local database file in turn takes precedence over the site database file.

Note:

- **- IF -** GDM is not installed on the system, this section can be skipped
- The Remediation Procedure commands in this section **MUST** be done from a command window on a graphical desktop or an error will be returned.

1.7.1 Ensure GDM is removed (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

Rationale:

If a Graphical User Interface (GUI) is not required, it should be removed to reduce the attack surface of the system.

Impact:

Removing the GNOME Display manager will remove the Graphical User Interface (GUI) from the system.

Audit:

Run the following command and verify `gdm3` is not installed:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' gdm3

gdm3       unknown ok not-installed        not-installed
```

Remediation:

Run the following commands to uninstall `gdm3` and remove unused dependencies:

```
# apt purge gdm3
# apt autoremove gdm3
```

References:

1. NIST SP 800-53 Rev. 5: CM-11

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1543, T1543.002	TA0002	M1033

1.7.2 Ensure GDM login banner is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

Audit:

Run the following commands to verify that the text banner on the login screen is enabled and set:

```
# gsettings get org.gnome.login-screen banner-message-enable
true
# gsettings get org.gnome.login-screen banner-message-text
'Authorized uses only. All activity may be monitored and reported'
```

Remediation:

- IF - A user profile is already created run the following commands to set and enable the text banner message on the login screen:

```
# gsettings set org.gnome.login-screen banner-message-text 'Authorized uses
only. All activity may be monitored and reported'
# gsettings set org.gnome.login-screen banner-message-enable true
```

Note:

- `banner-message-text` may be set in accordance with local site policy
- `gsettings` commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all `gsettings` configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF - A user profile does not exist:

1. Create or edit the gdm profile in the `/etc/dconf/profile/gdm` with the following lines:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Note: gdm is the name of a dconf database.

2. Create a gdm keyfile for machine-wide settings in `/etc/dconf/db/gdm.d/01-banner-message`:

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='Type the banner message here.'
```

3. Update the system databases

```
# dconf update
```

Note:

- Users must log out and back in again before the system-wide settings take effect.
- There is no character limit for the banner message. gnome-shell autodetects longer stretches of text and enters two column mode.
- The banner message cannot be read from an external file.

Default Value:

disabled

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/login-banner.html.en
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Additional Information:

Additional options and sections may appear in the `/etc/dconf/db/gdm.d/01-banner-message` file.

If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1087, T1087.001, T1087.002	TA0007	M1028

1.7.3 Ensure GDM disable-user-list option is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

The `disable-user-list` option controls if a list of users is displayed on the login screen

Rationale:

Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Audit:

Run the following command and to verify that the `disable-user-list` option is enabled:

```
# gsettings get org.gnome.login-screen disable-user-list
true
```

Remediation:

- IF - A user profile exists run the following command to enable the `disable-user-list`:

```
# gsettings set org.gnome.login-screen disable-user-list true
```

Note:

- `gsettings` commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all `gsettings` configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF - A user profile does not exist:

1. Create or edit the gdm profile in `/etc/dconf/profile/gdm` with the following lines:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Note: gdm is the name of a dconf database.

2. Create a gdm keyfile for machine-wide settings in `/etc/dconf/db/gdm.d/00-login-screen`:

```
[org/gnome/login-screen]
# Do not show the user list
disable-user-list=true
```

3. Update the system databases:

```
# dconf update
```

Note: When the user profile is created or changed, the user will need to log out and log in again before the changes will be applied.

Default Value:

false

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/login-userlist-disable.html.en
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Additional Information:

If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the user list

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1087, T1087.001, T1087.002	TA0007	M1028

1.7.4 Ensure GDM screen locks when the user is idle (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

Rationale:

Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

Audit:

Run the following commands to verify that the screen locks when the user is idle:

```
# gsettings get org.gnome.desktop.screensaver lock-delay
uint32 5
# gsettings get org.gnome.desktop.session idle-delay
uint32 900
```

Notes:

- `lock-delay=uint32 {n}` - should be 5 seconds or less and follow local site policy
- `idle-delay=uint32 {n}` - Should be 900 seconds (15 minutes) or less, not `0` (disabled) and follow local site policy

Remediation:

- IF - A user profile is already created run the following commands to enable screen locks when the user is idle:

```
# gsettings set org.gnome.desktop.screensaver lock-delay 5
# gsettings set org.gnome.desktop.session idle-delay 900
```

Note:

- `gsettings` commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all `gsettings` configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF- A user profile does not exist:

1. Create or edit the user profile in the `/etc/dconf/profile/` and verify it includes the following:

```
user-db:user
system-db:{NAME_OF_DCONF_DATABASE}
```

Note: `local` is the name of a dconf database used in the examples.

2. Create the directory `/etc/dconf/db/local.d/` if it doesn't already exist:
3. Create the key file `/etc/dconf/db/local.d/00-screensaver` to provide information for the `local` database:

Example key file:

```
# Specify the dconf path
[org/gnome/desktop/session]

# Number of seconds of inactivity before the screen goes blank
# Set to 0 seconds if you want to deactivate the screensaver.
idle-delay=uint32 180

# Specify the dconf path
[org/gnome/desktop/screensaver]

# Number of seconds after the screen is blank before locking the screen
lock-delay=uint32 0
```

Note: You must include the uint32 along with the integer key values as shown.

4. Run the following command to update the system databases:

```
# dconf update
```

5. Users must log out and back in again before the system-wide settings take effect.

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreen.html.en

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1461	TA0027	M1012

1.7.5 Ensure GDM screen locks cannot be overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GNOME Desktop Manager can lock down specific settings by using the lockdown mode in dconf to prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

Rationale:

Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

Without locking down the system settings, user settings take precedence over the system settings.

Audit:

Run the following script to verify that the screen lock cannot be overridden:

```
#!/usr/bin/env bash

{
   a_output=() a_output2=()
   f_check_setting()
   {
      grep -Psrilq -- "^\h*$2\b" /etc/dconf/db/local.d/locks/* && \
      echo "- \"$3\" is locked" || echo "- \"$3\" is not locked or not set"
   }
   declare -A settings=(
      ["idle-delay"]="/org/gnome/desktop/session/idle-delay"
      ["lock-delay"]="/org/gnome/desktop/screensaver/lock-delay"
   )
   for setting in "${!settings[@]}"; do
      result=$(f_check_setting "$setting" "${settings[$setting]}" "$setting")
      if [[ $result == *"is not locked"* || $result == *"not set to false"*
]]; then
         a_output2+=("$result")
      else
         a_output+=("$result")
      fi
   done
   printf '%s\n' "" "- Audit Result:"
   if [ "${#a_output2[@]}" -gt 0 ]; then
      printf '%s\n' "  ** FAIL **" " - Reason(s) for audit failure:"
"${a_output2[@]}"
      [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}"
   else
      printf '%s\n' "  ** PASS **" "${a_output[@]}"
   fi
}
```

Remediation:

1. To prevent the user from overriding these settings, create the file `/etc/dconf/db/local.d/locks/00-screensaver` with the following content:

```
# Lock desktop screensaver settings
/org/gnome/desktop/session/idle-delay
/org/gnome/desktop/screensaver/lock-delay
```

2. Update the system databases:

```
# dconf update
```

Note:

- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreen.html.en
2. https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en
3. NIST SP 800-53 Rev. 5: CM-11

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1456	TA0027	M1001

1.7.6 Ensure GDM automatic mounting of removable media is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

By default GNOME automatically mounts removable media when inserted as a convenience to the user.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

Audit:

Run the following commands to verify automatic mounting is disabled:

```
# gsettings get org.gnome.desktop.media-handling automount
false
# gsettings get org.gnome.desktop.media-handling automount-open
false
```

Remediation:

- IF - A user profile exists run the following commands to ensure automatic mounting is disabled:

```
# gsettings set org.gnome.desktop.media-handling automount false
# gsettings set org.gnome.desktop.media-handling automount-open false
```

Note:

- `gsettings` commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all `gsettings` configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF - A user profile does not exist:

1. Create a file `/etc/dconf/db/local.d/00-media-automount` with following content:

```
[org/gnome/desktop/media-handling]
automount=false
automount-open=false
```

2. After creating the file, apply the changes using below command :

```
# dconf update
```

Note: Users must log out and back in again before the system-wide settings take effect.

References:

1. https://access.redhat.com/solutions/20107
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0008	M1042

1.7.7 Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

By default GNOME automatically mounts removable media when inserted as a convenience to the user.

By using the lockdown mode in dconf, you can prevent users from changing specific settings. To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users

Audit:

Run the following script to verify automatic mounting of removable media is not overridden and correctly configured in a configuration file:

- `automount=false`
- `automount-open=false`

```
#!/usr/bin/env bash

{
   a_output=() a_output2=()
   check_setting()
   {
      grep -Psrilq "^\h*$1\h*=\h*false\b" /etc/dconf/db/local.d/locks/* 2>
/dev/null && \
      echo "- \"$3\" is locked and set to false" || echo "- \"$3\" is not
locked or not set to false"
   }
   declare -A settings=(
      ["automount"]="org/gnome/desktop/media-handling"
      ["automount-open"]="org/gnome/desktop/media-handling"
   )
   for setting in "${!settings[@]}"; do
      result=$(check_setting "$setting" "${settings[$setting]}" "$setting")
      if [[ $result == *"is not locked"* || $result == *"not set to false"*
]]; then
         a_output2+=("$result")
      else
         a_output+=("$result")
      fi
   done
   printf '%s\n' "" "- Audit Result:"
   if [ "${#a_output2[@]}" -gt 0 ]; then
      printf '%s\n' "  ** FAIL **" " - Reason(s) for audit failure:"
"${a_output2[@]}"
      [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}"
   else
      printf '%s\n' "  ** PASS **" "${a_output[@]}"
   fi
}
```

Remediation:

1. To prevent the user from overriding these settings, create the file `/etc/dconf/db/local.d/locks/00-media-automount` with the following content:

```
[org/gnome/desktop/media-handling]
automount=false
automount-open=false
```

2. Update the systems databases:

```
# dconf update
```

Note:

- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5
3. https://manpages.ubuntu.com/manpages/trusty/man1/gsettings.1.html
4. https://access.redhat.com/solutions/20107

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0001, TA0008	M1042

1.7.8 Ensure GDM autorun-never is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `autorun-never` setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

Rationale:

Malware on removable media may taking advantage of Autorun features when the media is inserted into a system and execute.

Audit:

Run the following command to verify that `autorun-never` is set to `true` for GDM:

```
# gsettings get org.gnome.desktop.media-handling autorun-never
true
```

Remediation:

- IF - A user profile exists run the following command to set `autorun-never` to `true` for GDM users:

```
# gsettings set org.gnome.desktop.media-handling autorun-never true
```

Note:

- `gsettings` commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all `gsettings` configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF - A user profile does not exist:

1. create the file `/etc/dconf/db/local.d/locks/00-media-autorun` with the following content:

```
[org/gnome/desktop/media-handling]
autorun-never=true
```

2. Update the systems databases:

```
# dconf update
```

Note: Users must log out and back in again before the system-wide settings take effect.

Default Value:

false

References:

1. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0001, TA0008	M1042

1.7.9 Ensure GDM autorun-never is not overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

By using the lockdown mode in dconf, you can prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

Rationale:

Malware on removable media may taking advantage of Autorun features when the media is inserted into a system and execute.

Audit:

Run the following script to verify that `autorun-never=true` cannot be overridden:

```
#!/usr/bin/env bash

{
    # Function to check and report if a specific setting is locked and set to
true
    check_setting() {
        grep -Psrilq "^\h*$1\h*=\h*true\b" /etc/dconf/db/local.d/locks/* 2>
/dev/null && echo "- \"$3\" is locked and set to false" || echo "- \"$3\" is
not locked or not set to false"
    }
    # Array of settings to check
    declare -A settings=(["autorun-never"]="org/gnome/desktop/media-
handling")
    # Check GNOME Desktop Manager configurations
    l_output=() l_output2=()
    for setting in "${!settings[@]}"; do
        result=$(check_setting "$setting")
        l_output+=("$result")
        if [[ $result == *"is not locked"* || $result == *"not set to true"*
]]; then
            l_output2+=("$result")
        fi
    done
    # Report results
    if [ ${#l_output2[@]} -ne 0 ]; then
        printf '%s\n' "- Audit Result:" "  ** FAIL **"
        printf '%s\n' "- Reason(s) for audit failure:"
        for msg in "${l_output2[@]}"; do
            printf '%s\n' "$msg"
        done
    else
        printf '%s\n' "- Audit Result:" "  ** PASS **"
    fi
}
```

Remediation:

1. To prevent the user from overriding these settings, create the file `/etc/dconf/db/local.d/locks/00-media-autorun` with the following content:

```
[org/gnome/desktop/media-handling]
autorun-never=true
```

2. Update the systems databases:

```
# dconf update
```

Note:

- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.

References:

1. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0001, TA0008	M1028

1.7.10 Ensure XDMCP is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays

Rationale:

XDMCP is inherently insecure.

- XDMCP is not a ciphered protocol. This may allow an attacker to capture keystrokes entered by a user
- XDMCP is vulnerable to man-in-the-middle attacks. This may allow an attacker to steal the credentials of legitimate users by impersonating the XDMCP server.

Audit:

Run the following script and verify the output:

```
#!/usr/bin/env bash

{
   while IFS= read -r l_file; do
      awk '/\[xdmcp\]/{ f = 1;next } /\[/{ f = 0 } f {if
(/^\s*Enable\s*=\s*true/) print "The file: \"'"$l_file"'\" includes: \"" $0
"\" in the \"[xdmcp]\" block"}' "$l_file"
   done < <(grep -Psil -- '^\h*\[xdmcp\]'
/etc/{gdm3,gdm}/{custom,daemon}.conf)
}
```

Nothing should be returned

Remediation:

Edit all files returned by the audit and remove or commend out the `Enable=true` line in the `[xdmcp]` block:
Example file:

```
# GDM configuration storage
#
# See /usr/share/gdm/gdm.schemas for a list of available options.

[daemon]
# Uncomment the line below to force the login screen to use Xorg
#WaylandEnable=false

# Enabling automatic login
#  AutomaticLoginEnable = true
#  AutomaticLogin = user1

# Enabling timed login
#  TimedLoginEnable = true
#  TimedLogin = user1
#  TimedLoginDelay = 10

[security]

[xdmcp]
# Enable=true <- **This line should be removed or commented out**

[chooser]

[debug]
# Uncomment the line below to turn on debugging
# More verbose logs
# Additionally lets the X server dump core if it crashes
#Enable=true
```

Default Value:

false (This is denoted by no Enabled= entry in the [xdmcp] block

References:

1. NIST SP 800-53 Rev. 5: SI-4

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1056, T1056.001, T1557, T1557.000	TA0002	M1050