

INTEROFFICE MEMORANDUM

To: Management

From: Team

Subject: Login Banner Improvements

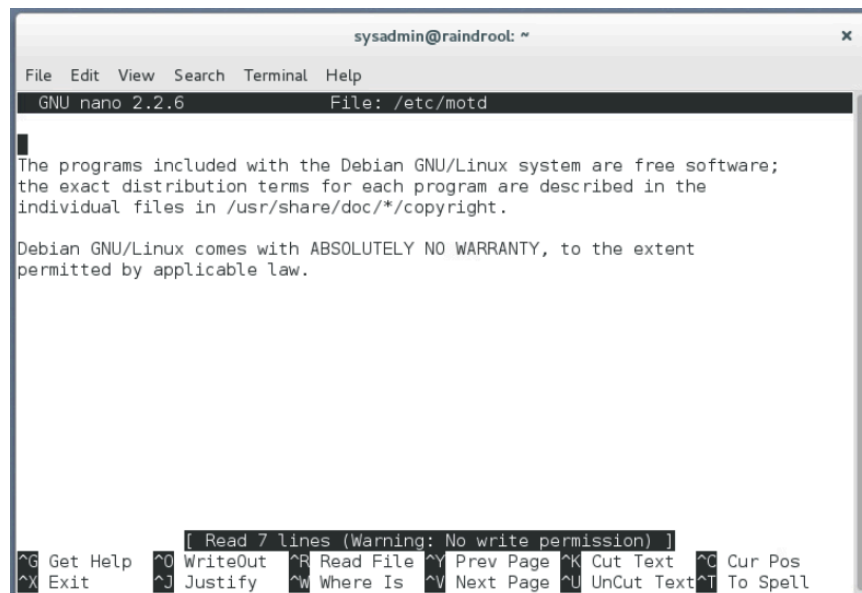
Date:

Management,

Thank you for expressing your concern regarding our computer systems' login banners.

We have taken steps to correct this shortcoming by modifying login banners on our devices so that when someone logs in to access a device they are informed of our company's acceptable use and security monitoring actions. Due to the Computer Fraud and Abuse Act, when someone unauthorized accesses one of our devices, they can now be prosecuted for the unauthorized access because they are warned about accessing devices without authorization.

Previously login banners on our systems looked like this:

A screenshot of a terminal window titled 'sysadmin@raindrool: ~'. The window shows the GNU nano 2.2.6 editor editing the file /etc/motd. The content of the file is a standard Ubuntu login banner. The banner text reads: 'The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright. Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.' The terminal window has a menu bar with 'File Edit View Search Terminal Help' and a status bar at the bottom with various keyboard shortcuts like '^G Get Help', '^O WriteOut', '^R Read File', etc. A warning message '[Read 7 lines (Warning: No write permission)]' is visible above the status bar.

```
sysadmin@raindrool: ~
File Edit View Search Terminal Help
GNU nano 2.2.6 File: /etc/motd

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

[ Read 7 lines (Warning: No write permission) ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

Figure 1. Ubuntu initial login banner

```
[root@splunk ~]# cat /etc/motd

-----
As user "root",
Use "dcn-network-config" to (re)configure networking.
Use "dcn-network-config --help" to get help for command line arguments.
Use "dcn-splunk-config" to (re)configure Splunk.
-----

[root@splunk ~]# _
```

Figure 2. Splunk with no initial login banner

Our previous login banners provided information about our systems including the operating system in use. Our new login banners reference the company Acceptable Use Policy and emphasize the ability to prosecute misuse or unauthorized access.

New Login Banner:

```
***** WARNING *****

This system is the property of a private organization and is for authorized use
only. By accessing this system, users agree to comply with the company's
Acceptable Use Policy.

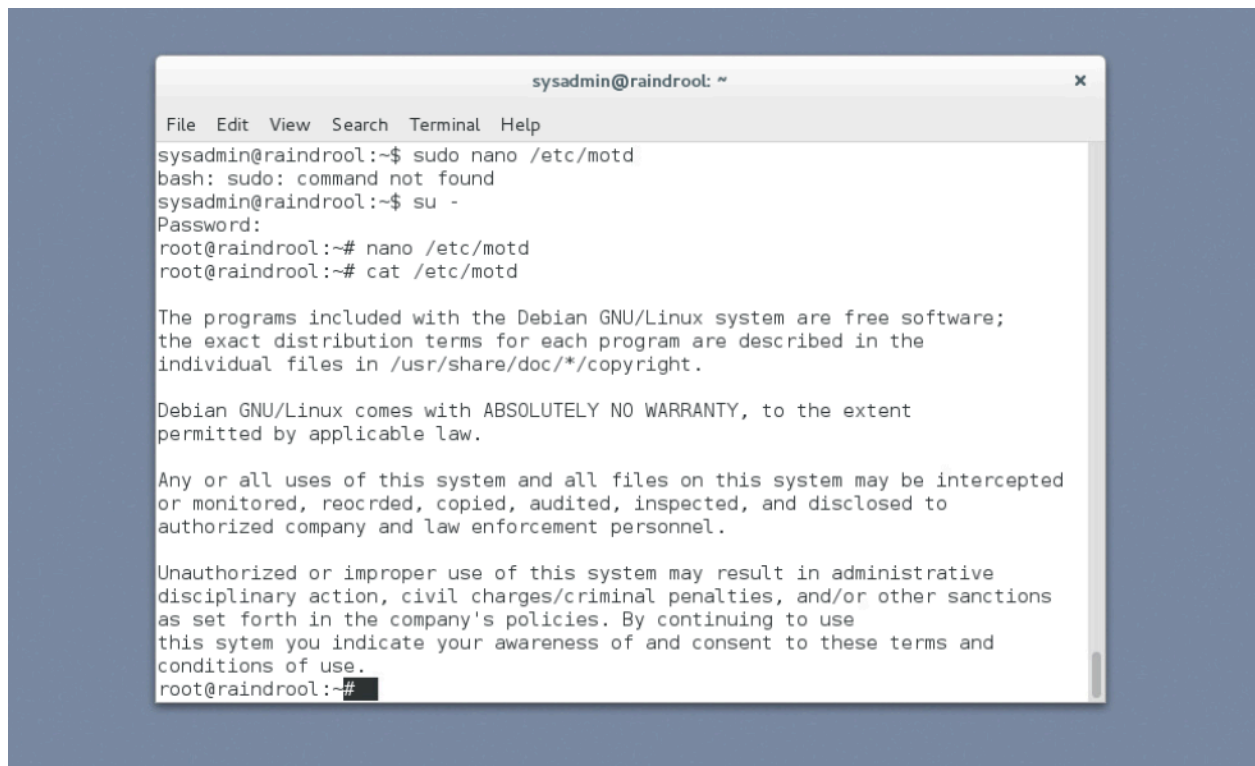
All activities on this system may be monitored, recorded, and disclosed to
authorized personnel for security purposes. There is no expectation of privacy
while using this system.

Unauthorized or improper use may result in disciplinary action or legal
penalties. By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use.

*****
```

Figure 3. New Login Banner

The new login banner has successfully been installed on our machines and is evident in the images below:

A screenshot of a terminal window titled 'sysadmin@raindroot: ~'. The terminal shows a sequence of commands and their outputs. First, 'sysadmin@raindroot:~\$ sudo nano /etc/motd' is entered, resulting in 'bash: sudo: command not found'. Then, 'sysadmin@raindroot:~\$ su -' is entered, followed by a password prompt. After logging in as root, 'root@raindroot:~# nano /etc/motd' and 'root@raindroot:~# cat /etc/motd' are entered. The output of 'cat /etc/motd' displays the Debian GNU/Linux login banner, which includes information about free software, warranty, and system usage policies.

```
sysadmin@raindroot: ~
File Edit View Search Terminal Help
sysadmin@raindroot:~$ sudo nano /etc/motd
bash: sudo: command not found
sysadmin@raindroot:~$ su -
Password:
root@raindroot:~# nano /etc/motd
root@raindroot:~# cat /etc/motd

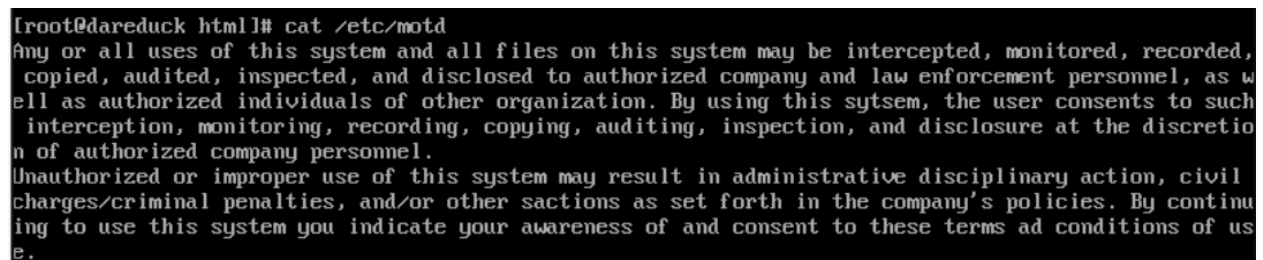
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Any or all uses of this system and all files on this system may be intercepted
or monitored, reocrded, copied, audited, inspected, and disclosed to
authorized company and law enforcement personnel.

Unauthorized or improper use of this system may result in administrative
disciplinary action, civil charges/criminal penalties, and/or other sanctions
as set forth in the company's policies. By continuing to use
this sytem you indicate your awareness of and consent to these terms and
conditions of use.
root@raindroot:~#
```

Figure 4. Debian Login Banner

A screenshot of a terminal window showing the output of the 'cat /etc/motd' command. The output displays the CentOS 7 login banner, which includes information about system usage, interception, and consent to terms and conditions.

```
[root@dareduck html]# cat /etc/motd
Any or all uses of this system and all files on this system may be intercepted, monitored, recorded,
copied, audited, inspected, and disclosed to authorized company and law enforcement personnel, as w
ell as authorized individuals of other organization. By using this sytsem, the user consents to such
interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretio
n of authorized company personnel.
Unauthorized or improper use of this system may result in administrative disciplinary action, civil
charges/criminal penalties, and/or other sactions as set forth in the company's policies. By continu
ing to use this system you indicate your awareness of and consent to these terms ad conditions of us
e.
```

Figure 5. CentOS 7 Login Banner

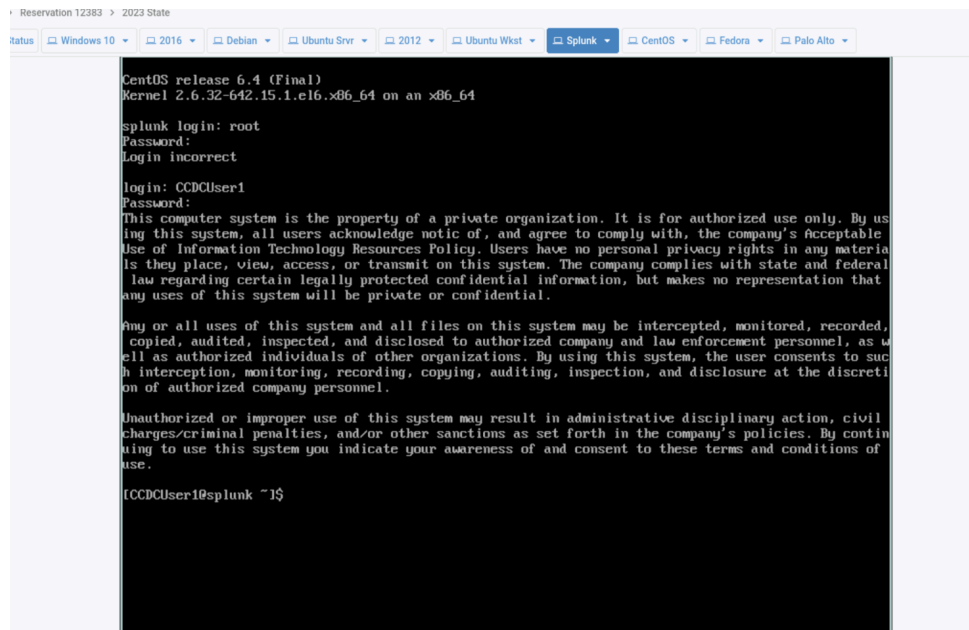


Figure 6. Splunk Login Banner Updated

```

GNU nano 2.2.6      File: /etc/update-motd.d/00-header

#!/bin/sh
#
# 00-header - create the header of the MOTD
# Copyright (C) 2009-2010 Canonical Ltd.
#
# Authors: Dustin Kirkland <kirkland@canonical.com>
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License along
# with this program; if not, write to the Free Software Foundation, Inc.,
# 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release

if [ -z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then
    # Fall back to using the very slow lsb_release utility
    DISTRIB_DESCRIPTION=$(lsb_release -s -d)
fi

printf "Any or all uses of this system and all files on this system may be intercepted, monitored, $
printf "Unauthorized or improper use of this system may result in administrative disciplinary actio$

```

Figure 7. Ubuntu Server Login Banner

Windows Devices Login Banner

For Windows devices' login banners, the message title was set to "Warning" and the message text to "This computer should be used for authorized purposes only. Unauthorized use of this computer will lead to disciplinary action or prosecution." Whenever a user logs on to a Windows system, this interactive message is displayed. This was **applied to all devices on the Windows Domain through a Group Policy**. The user can then log in by clicking on the OK button.

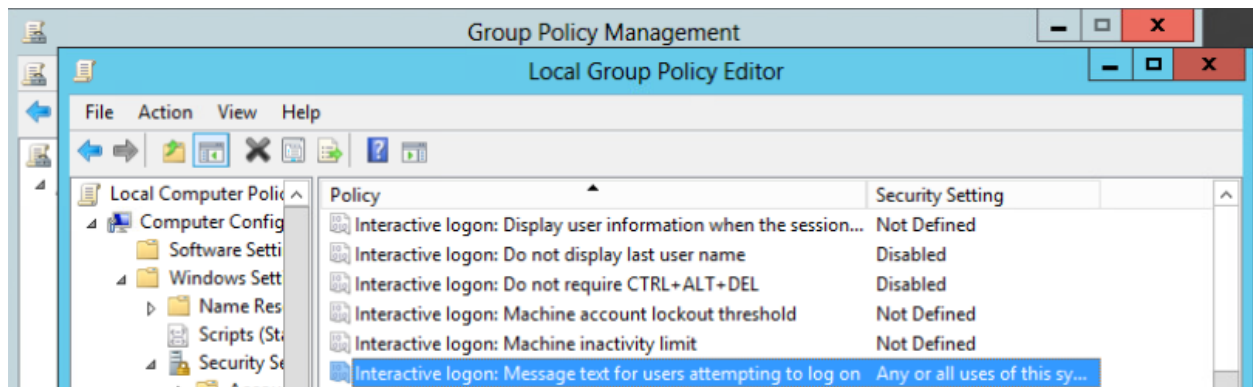


Figure 9. Windows Login Banner set for Domain

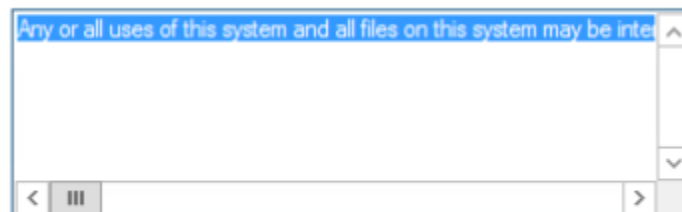


Figure 10. Windows Login Message

Please let us know if there are any additional actions the security team can perform to improve the login banners.

Thank you,

Team