Linux Log Files 01

This presentation uses Kali 1.0.6 for three examples and OpenSUSE 13.1 for one example of log file capture. Kali example collects a failed login, failed file access, and failed privilege service stop. OpenSUSE example shows a firewall log.

Preuss
2/20/2014

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:20 AM root

Computer

Kali Live

The presentation logs into Kali as root.

KALI LINUX

The quieter you become, the more you are able to hear.

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:20 AM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#

The presentation opens a terminal window on Kali.

KALI LINUX

The quieter you become, the more you are able to hear.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:21 AM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# adduser alphonse
```

The presentation creates a login for Alphonse Albatross.

KALI LINUX

The quieter you become, the more you are able to hear.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:21 AM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# adduser alphonse
Adding user `alphonse' ...
Adding new group `alphonse' (1002) ...
Adding new user `alphonse' (1001) with group `alphonse' ...
Creating home directory `/home/alphonse' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for alphonse
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
```

The presentation finishes creating the login by answering Y to the final question.

KALI LINUX

The quieter you become, the more you are able to hear.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Thu 3:22 AM

kali

alphonse

Password:

System Default

Cancel

Log In

The presentation intentionally fails to login to Kali.

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:24 AM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# cat /var/log/auth.log | grep alphonse
Feb 20 03:21:13 kali groupadd[3206]: group added to /etc/group: name=alphonse, G
ID=1002
Feb 20 03:21:13 kali groupadd[3206]: group added to /etc/gshadow: name=alphonse
Feb 20 03:21:13 kali groupadd[3206]: new group: name=alphonse, GID=1002
Feb 20 03:21:13 kali useradd[3210]: new user: name=alphonse, UID=1001, GID=1002,
 home=/home/alphonse, shell=/bin/bash
Feb 20 03:21:37 kali passwd[3218]: pam_unix(passwd:chauthtok): password changed
for alphonse
Feb 20 03:21:45 kali chfn[3219]: changed user 'alphonse' information
Feb 20 03:22:29 kali gdm3][3306]: pam_unix(gdm3:auth): authentication failure; l
ogname= uid=0 euid=0 tty=:0 ruser= rhost=  user=alphonse
root@kali:~#
```

The presentation logs on Kali Linux as root. The presentation opens a terminal window. The presentation searches /var/log/auth.log for the failed login. The last entry is the failed login.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:27 AM alphonse

Computer

Kali Live

alphonse@kali: ~

File Edit View Search Terminal Help

```
alphonse@kali:~$ cat /etc/shadow
```

The presentation logs in as Alphonse. The presentation as Alphonse tries to view /etc/shadow as shown.

alphonse@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:27 AM alphonse

Computer

Kali Live

alphonse@kali: ~

File Edit View Search Terminal Help

```
alphonse@kali:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
alphonse@kali:~$
```

The presentation as Alphonse receives the expected message.

alphonse@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:28 AM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# cat /var/log/auth.log | grep alphonse
Feb 20 03:21:13 kali groupadd[3206]: group added to /etc/group: name=alphonse, G
ID=1002
Feb 20 03:21:13 kali groupadd[3206]: group added to /etc/gshadow: name=alphonse
Feb 20 03:21:13 kali groupadd[3206]: new group: name=alphonse, GID=1002
Feb 20 03:21:13 kali useradd[3210]: new user: name=alphonse, UID=1001, GID=1002,
 home=/home/alphonse, shell=/bin/bash
Feb 20 03:21:37 kali passwd[3218]: pam_unix(passwd:chauthtok): password changed
for alphonse
Feb 20 03:21:45 kali chfn[3219]: changed user 'alphonse' information
Feb 20 03:22:29 kali gdm3][3306]: pam_unix(gdm3:auth): authentication failure; l
ogname= uid=0 euid=0 tty=:0 ruser= rhost=  user=alphonse
Feb 20 03:25:07 kali gdm3][3674]: pam_unix(gdm3:session): session opened for use
r alphonse by (uid=0)
Feb 20 03:25:07 kali gnome-keyring-daemon[3678]: couldn't bind to control socket
: /home/alphonse/.cache/keyring-3Ds5bz/control: No such file or directory
root@kali:~#
```

The presentation logs in to Kali as root. The presentation opens a terminal window. The presentation searches /var/log/auth.log for the failed file access. The last line shown is the failed file access.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 3:33 AM alphonse

Computer

Kali Live

alphonse@kali: ~

File Edit View Search Terminal Help

```
alphonse@kali:~$ ps aux
```

The presentation logs in as Alphonse. The presentation generates a list of process status.

KALI LINUX

The quieter you become, the more you are able to hear.

alphonse@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 4:22 AM alphonse

Computer

Kali Live

alphonse@kali: ~

File Edit View Search Terminal Help

```
root      2719  0.0  0.3  34560  3796 ?        Sl   04:17   0:00 /usr/lib/upower/upowerd
rtkit     2900  0.0  0.1  18988  1224 ?        SNl  04:17   0:00 /usr/lib/rtkit/rtkit-daemo
root      2932  0.0  0.3  26808  4056 ?        Sl   04:18   0:00 gdm-session-worker [pam/gd
alphonse  2939  0.0  0.3  59840  4032 ?        Sl   04:18   0:00 /usr/bin/gnome-keyring-dae
root      2941  0.0  0.0      0     0 ?        S    04:18   0:00 [kauditd]
alphonse  2957  0.0  0.8  48956  9040 ?        Ssl  04:18   0:00 x-session-manager
alphonse  2999  0.0  0.0   3516   532 ?        S    04:18   0:00 dbus-launch --autolaunch=7
alphonse  3000  0.0  0.0   3012   924 ?        Ss   04:18   0:00 /usr/bin/dbus-daemon --for
alphonse  3003  0.0  0.2  30332  2400 ?        Sl   04:18   0:00 /usr/lib/dconf/dconf-servi
alphonse  3016  0.0  0.0   3868   212 ?        Ss   04:18   0:00 /usr/bin/ssh-agent /usr/bi
alphonse  3019  0.0  0.0   3516   532 ?        S    04:18   0:00 /usr/bin/dbus-launch --exi
alphonse  3020  0.0  0.1   4468  1764 ?        Ss   04:18   0:00 /usr/bin/dbus-daemon --for
alphonse  3027  0.1  1.3 152456 14428 ?        Sl   04:18   0:00 /usr/lib/gnome-settings-da
alphonse  3035  0.0  0.2   8552  2424 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd
alphonse  3044  0.1  0.5  97516  5680 ?        S<l  04:18   0:00 /usr/bin/pulseaudio --star
alphonse  3048  0.0  0.3  33996  3796 ?        S    04:18   0:00 /usr/lib/gvfs/gvfs-gdu-vol
root      3050  0.0  0.3  22968  3404 ?        Sl   04:18   0:00 /usr/lib/udisks/udisks-dae
root      3051  0.0  0.0   6352   724 ?        S    04:18   0:00 udisks-daemon: polling /de
alphonse  3054  0.0  0.2   8600  2176 ?        S    04:18   0:00 /usr/lib/gvfs/gvfs-gphoto2
alphonse  3056  0.0  0.2  19068  2356 ?        Sl   04:18   0:00 /usr/lib/gvfs/gvfs-afc-vol
colord    3060  0.0  0.4  24584  4264 ?        Sl   04:18   0:00 /usr/lib/i386-linux-gnu/co
root      3061  0.0  0.5  55732  5648 ?        Sl   04:18   0:00 /usr/lib/packagekit/packag
alphonse  3062  0.0  1.0 115908 11268 ?        Sl   04:18   0:00 /usr/bin/metacity
alphonse  3064  0.0  0.3  4626                                  /lib/gnome-settings-da
```

The presentation as Alphonse decides to stop the process 3061 owned by root.

alphonse@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 4:22 AM alphonse

Computer

Kali Live

alphonse@kali: ~

File Edit View Search Terminal Help

```
colord    3078  0.0  0.7  34232  7812 ?        Sl   04:18   0:00 /usr/lib/i386-linux-gnu/co
alphonse  3090  0.0  0.2   8328  2768 ?        S    04:18   0:00 /usr/lib/i386-linux-gnu/gc
alphonse  3092  0.0  0.2  30332  2412 ?        Sl   04:18   0:00 /usr/lib/dconf/dconf-servi
alphonse  3096  0.1  1.4  71784 15452 ?        Sl   04:18   0:00 nm-applet
alphonse  3097  0.0  0.8  39552  8492 ?        Sl   04:18   0:00 /usr/lib/notification-daem
alphonse  3098  0.0  0.8  24848  8308 ?        S    04:18   0:00 /usr/lib/gnome-disk-utilit
alphonse  3099  0.2  2.0  90712 21188 ?        Sl   04:18   0:00 nautilus -n
alphonse  3102  0.0  0.8  56048  8292 ?        Sl   04:18   0:00 /usr/lib/gnome-settings-da
alphonse  3104  0.0  0.8  40100  8352 ?        Sl   04:18   0:00 gnome-screensaver
alphonse  3113  0.0  1.1  54156 11644 ?        Sl   04:18   0:00 bluetooth-applet
alphonse  3116  0.0  0.7  31480  8016 ?        Sl   04:18   0:00 /usr/lib/policykit-1-gnome
alphonse  3117  0.0  0.7  49304  7888 ?        SNl  04:18   0:00 /usr/lib/tracker/tracker-m
alphonse  3126  0.0  1.3 115244 13680 ?        Sl   04:18   0:00 gnome-sound-applet
alphonse  3141  0.0  0.8  63808  8392 ?        Sl   04:18   0:00 /usr/lib/tracker/tracker-s
alphonse  3159  0.0  0.3   9080  3160 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd-trash
alphonse  3161  0.0  0.2   8552  2524 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd-burn -
alphonse  3164  0.0  0.5  37016  5220 ?        Sl   04:18   0:00 /usr/lib/telepathy/mission
alphonse  3169  0.0  0.9  92016  9576 ?        Sl   04:18   0:00 /usr/lib/gnome-online-acco
alphonse  3178  0.5  1.5  74512 16072 ?        Sl   04:18   0:01 gnome-terminal
alphonse  3185  0.0  0.0   2080   700 ?        S    04:18   0:00 gnome-pty-helper
alphonse  3186  0.0  0.3   6136  3452 pts/0    Ss   04:18   0:00 bash
alphonse  3304  0.0  0.1   4280  1188 pts/0
alphonse@kali:~$
alphonse@kali:~$ kill 3061
```

The presentation issues the command to stop the process owned by root.

alphonse@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 4:22 AM alphonse

Computer

Kali Live

alphonse@kali: ~

File Edit View Search Terminal Help

```
alphonse  3092  0.0  0.2  30332  2412 ?        Sl   04:18   0:00 /usr/lib/dconf/dconf-servi
alphonse  3096  0.1  1.4  71784 15452 ?        Sl   04:18   0:00 nm-applet
alphonse  3097  0.0  0.8  39552  8492 ?        Sl   04:18   0:00 /usr/lib/notification-daem
alphonse  3098  0.0  0.8  24848  8308 ?        S    04:18   0:00 /usr/lib/gnome-disk-utilit
alphonse  3099  0.2  2.0  90712 21188 ?        Sl   04:18   0:00 nautilus -n
alphonse  3102  0.0  0.8  56048  8292 ?        Sl   04:18   0:00 /usr/lib/gnome-settings-da
alphonse  3104  0.0  0.8  40100  8352 ?        Sl   04:18   0:00 gnome-screensaver
alphonse  3113  0.0  1.1  54156 11644 ?        Sl   04:18   0:00 bluetooth-applet
alphonse  3116  0.0  0.7  31480  8016 ?        Sl   04:18   0:00 /usr/lib/policykit-1-gnome
alphonse  3117  0.0  0.7  49304  7888 ?        SNl  04:18   0:00 /usr/lib/tracker/tracker-m
alphonse  3126  0.0  1.3 115244 13680 ?        Sl   04:18   0:00 gnome-sound-applet
alphonse  3141  0.0  0.8  63808  8392 ?        Sl   04:18   0:00 /usr/lib/tracker/tracker-s
alphonse  3159  0.0  0.3   9080  3160 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd-trash
alphonse  3161  0.0  0.2   8552  2524 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd-burn -
alphonse  3164  0.0  0.5  37016  5220 ?        Sl   04:18   0:00 /usr/lib/telepathy/mission
alphonse  3169  0.0  0.9  92016  9576 ?        Sl   04:18   0:00 /usr/lib/gnome-online-acco
alphonse  3178  0.5  1.5  74512 16072 ?        Sl   04:18   0:01 gnome-terminal
alphonse  3185  0.0  0.0   2080   700 ?        S    04:18   0:00 gnome-pty-helper
alphonse  3186  0.0  0.3   6136  3452 pts/0    Ss   04:18   0:00 bash
alphonse  3304  0.0  0.1   4280  1188 pts/0    R+   04:21   0:00 ps aux
alphonse@kali:~$
alphonse@kali:~$ kill 3061
bash: kill: (3061) - Operation not permitted
alphonse@kali:~$
```

KALI LINUX

The quieter you become, the more you

The presentation recieves the expected response.

alphonse@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 4:22 AM alphonse

Computer

Kali Live

root@kali: /home/alphonse

File Edit View Search Terminal Help

```
alphonse  3097  0.0  0.8  39552  8492 ?        Sl   04:18   0:00 /usr/lib/notification-daem
alphonse  3098  0.0  0.8  24848  8308 ?        S    04:18   0:00 /usr/lib/gnome-disk-utilit
alphonse  3099  0.2  2.0  90712 21188 ?        Sl   04:18   0:00 nautilus -n
alphonse  3102  0.0  0.8  56048  8292 ?        Sl   04:18   0:00 /usr/lib/gnome-settings-da
alphonse  3104  0.0  0.8  40100  8352 ?        Sl   04:18   0:00 gnome-screensaver
alphonse  3113  0.0  1.1  54156 11644 ?        Sl   04:18   0:00 bluetooth-applet
alphonse  3116  0.0  0.7  31480  8016 ?        Sl   04:18   0:00 /usr/lib/policykit-1-gnome
alphonse  3117  0.0  0.7  49304  7888 ?        SNl  04:18   0:00 /usr/lib/tracker/tracker-m
alphonse  3126  0.0  1.3 115244 13680 ?        Sl   04:18   0:00 gnome-sound-applet
alphonse  3141  0.0  0.8  63808  8392 ?        Sl   04:18   0:00 /usr/lib/tracker/tracker-s
alphonse  3159  0.0  0.3   9080  3160 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd-trash
alphonse  3161  0.0  0.2   8552  2524 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd-burn -
alphonse  3164  0.0  0.5  37016  5220 ?        Sl   04:18   0:00 /usr/lib/telepathy/mission
alphonse  3169  0.0  0.9  92016  9576 ?        Sl   04:18   0:00 /usr/lib/gnome-online-acco
alphonse  3178  0.5  1.5  74512 16072 ?        Sl   04:18   0:01 gnome-terminal
alphonse  3185  0.0  0.0   2080   700 ?        S    04:18   0:00 gnome-pty-helper
alphonse  3186  0.0  0.3   6136  3452 pts/0    Ss   04:18   0:00 bash
alphonse  3304  0.0  0.1   4280  1188 pts/0    R+   04:21   0:00 ps aux
alphonse@kali:~$
alphonse@kali:~$ kill 3061
bash: kill: (3061) - Operation not permitted
alphonse@kali:~$ su
Password:
root@kali:/home/alphonse#
```

The presentation becomes root to view the log files.

root@kali: /home/alph...

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 4:23 AM alphonse

Computer

Kali Live

root@kali: /home/alphonse

File Edit View Search Terminal Help

```
alphonse  3097  0.0  0.8  39552  8492 ?        Sl   04:18   0:00 /usr/lib/notification-daem
alphonse  3098  0.0  0.8  24848  8308 ?        S    04:18   0:00 /usr/lib/gnome-disk-utilit
alphonse  3099  0.2  2.0  90712 21188 ?        Sl   04:18   0:00 nautilus -n
alphonse  3102  0.0  0.8  56048  8292 ?        Sl   04:18   0:00 /usr/lib/gnome-settings-da
alphonse  3104  0.0  0.8  40100  8352 ?        Sl   04:18   0:00 gnome-screensaver
alphonse  3113  0.0  1.1  54156 11644 ?        Sl   04:18   0:00 bluetooth-applet
alphonse  3116  0.0  0.7  31480  8016 ?        Sl   04:18   0:00 /usr/lib/policykit-1-gnome
alphonse  3117  0.0  0.7  49304  7888 ?        SNl  04:18   0:00 /usr/lib/tracker/tracker-m
alphonse  3126  0.0  1.3 115244 13680 ?        Sl   04:18   0:00 gnome-sound-applet
alphonse  3141  0.0  0.8  63808  8392 ?        Sl   04:18   0:00 /usr/lib/tracker/tracker-s
alphonse  3159  0.0  0.3   9080  3160 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd-trash
alphonse  3161  0.0  0.2   8552  2524 ?        S    04:18   0:00 /usr/lib/gvfs/gvfsd-burn -
alphonse  3164  0.0  0.5  37016  5220 ?        Sl   04:18   0:00 /usr/lib/telepathy/mission
alphonse  3169  0.0  0.9  92016  9576 ?        Sl   04:18   0:00 /usr/lib/gnome-online-acco
alphonse  3178  0.5  1.5  74512 16072 ?        Sl   04:18   0:01 gnome-terminal
alphonse  3185  0.0  0.0   2080   700 ?        S    04:18   0:00 gnome-pty-helper
alphonse  3186  0.0  0.3   6136  3452 pts/0    Ss   04:18   0:00 bash
alphonse  3304  0.0  0.1   4280  1188 pts/0    R+   04:21   0:00 ps aux
alphonse@kali:~$
alphonse@kali:~$ kill 3061
bash: kill: (3061) - Operation not permitted
alphonse@kali:~$ su
Password:
root@kali:/home/alphonse# cat /var/log/auth.log
```

The presentation, as root, issues the command to view /var/log/auth.log

root@kali: /home/alph...

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Thu Feb 20, 4:23 AM alphonse

Computer

Kali Live

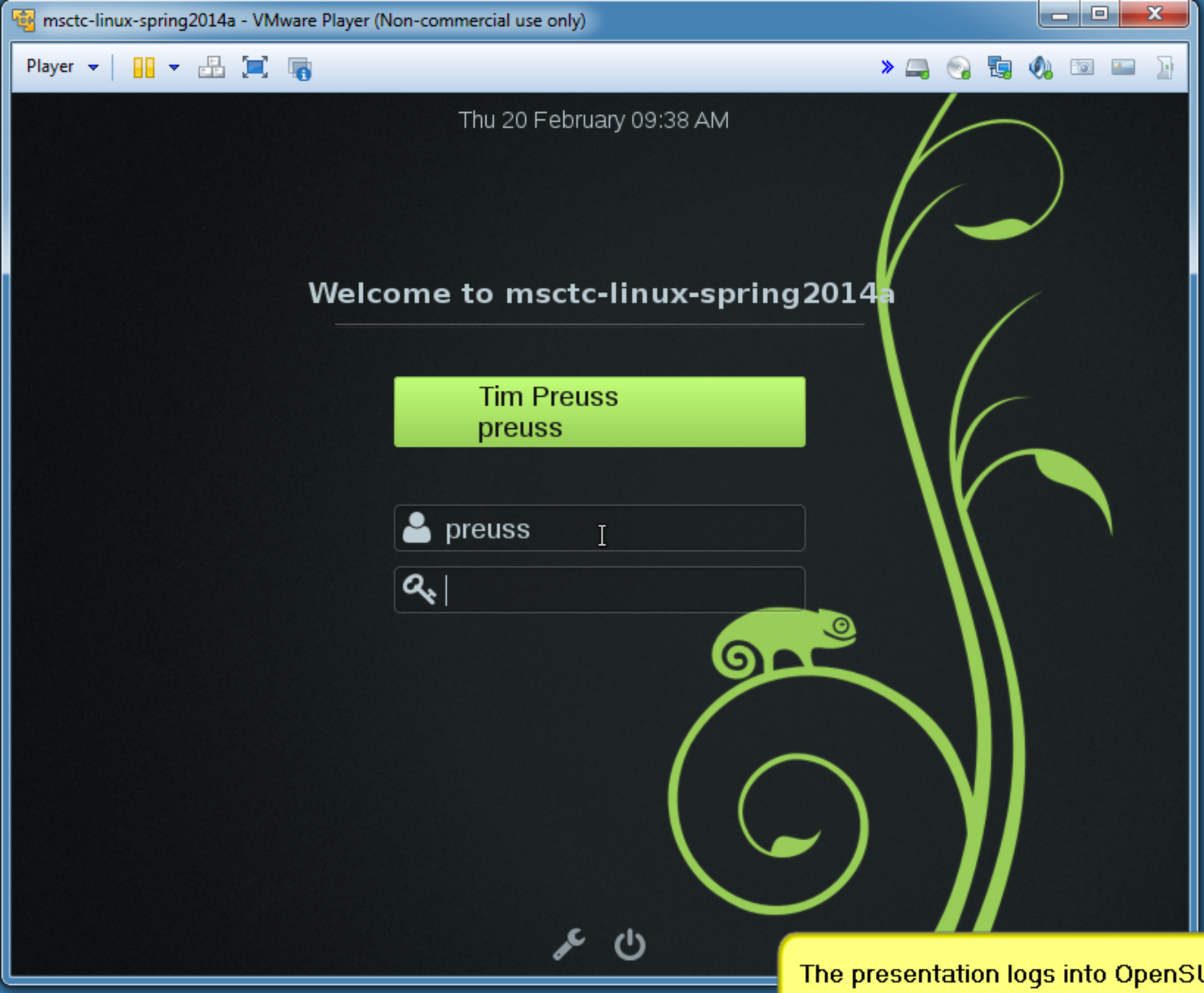
root@kali: /home/alphonse

File Edit View Search Terminal Help

```
="0" destination=":1.9" (uid=0 pid=2621 comm="/usr/sbin/console-kit-daemon --no-daemon ")
Feb 20 04:18:13 kali gdm3][2932]: pam_unix(gdm3:session): session opened for user alphonse
by (uid=0)
Feb 20 04:18:13 kali gdm3][2932]: pam_ck_connector(gdm3:session): nox11 mode, ignoring PAM_
TTY :0
Feb 20 04:18:13 kali gdm-welcome][2612]: pam_unix(gdm-welcome:session): session closed for
user Debian-gdm
Feb 20 04:18:13 kali polkitd(authority=local): Unregistered Authentication Agent for unix-s
ession:/org/freedesktop/ConsoleKit/Session1 (system bus name :1.26, object path /org/gnome/
PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
```

The log entry Feb 20 04:18:13 shows the failure. This is shown by disconnection from the bus

root@kali: /home/alph...



The presentation logs into OpenSUSE 13.1

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

Firefox

KInfoCenter

Office

Online Help

openSU

YaST Control Center @ msctc-linux-spring2014a

Search

Software

Hardware

System

Network Devices

Network Services

Security and Users

Support

Miscellaneous

Software

Add-On Products

Media Check

Online Update

Online Update Configuration

Software Management

Software Repositories

Hardware

Hardware Information

Ready

The presentation opens YaST.

YaST Control Center @ msctc-lir

1

09:41 AM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

Firefox

KInfoCenter

Office

Online Help

openSU

YaST Control Center @ msctc-linux-spring2014a

Search

Software

Hardware

System

Network Devices

Network Services

Security and Users

Support

Miscellaneous

Security and Users

AppArmor Configuration

YaST2

Start-Up
Interfaces
Allowed Services
Masquerading
Broadcast
Logging Level
Custom Rules

Firewall Configuration: Logging Level

Logging Level

Logging Accepted Packets

Log Only Critical

Logging Not Accepted Packets

Log Only Critical

The presentation opens the YaST firewall configuration. The configuration shown will work in many cases. It is possible to log all packets to be sure.

Help

Cancel

Back

Next

YaST Control Center @ msctc-lir

YaST2

1

09:42 AM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

Firefox

KInfoCenter

Office

Online Help

openSU

preuss : bash - Konsole

File Edit View Bookmarks Settings Help

```
msctc-linux-spring2014a:/home/preuss #
```

preuss : bash

The presentation opens the command prompt. The presentation becomes root, as shown.

preuss : bash – Konsole

1

09:43 AM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

Firefox

KInfoCenter

Office

Online Help

openSU

preuss : bash - Konsole

File Edit View Bookmarks Settings Help

```
msctc-linux-spring2014a:/home/preuss # cat /var/log/firewall | grep DROP
```

preuss : bash

The presentation searches the /var/log/firewall for dropped packets.

preuss : bash - Konsole

1

09:44 AM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

Firefox

KInfoCenter

Office

Online Help

openSU

preuss : bash - Konsole

File Edit View Bookmarks Settings Help

```
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=557 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP
SPT=5353 DPT=5353 LEN=517
2014-02-20T09:38:28.179901-06:00 msctc-linux-spring2014a kernel: [   44.050954] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
2014-02-20T09:38:29.180867-06:00 msctc-linux-spring2014a kernel: [   45.052967] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
2014-02-20T09:38:31.183091-06:00 msctc-linux-spring2014a kernel: [   47.056957] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
2014-02-20T09:38:35.186064-06:00 msctc-linux-spring2014a kernel: [   51.063070] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
2014-02-20T09:38:43.187412-06:00 msctc-linux-spring2014a kernel: [   59.070673] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
2014-02-20T09:38:59.227772-06:00 msctc-linux-spring2014a kernel: [   75.111073] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
2014-02-20T09:39:31.240905-06:00 msctc-linux-spring2014a kernel: [  107.165731] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
2014-02-20T09:40:35.246666-06:00 msctc-linux-spring2014a kernel: [  171.228115] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
2014-02-20T09:42:43.300678-06:00 msctc-linux-spring2014a kernel: [  299.396580] SPW2-INext-DROP-DEFLT IN=eth0 OUT= MAC= SRC=fe8
0:0000:0000:0000:020c:29ff:fe80:bbc6 DST=ff02:0000:0000:0000:0000:0000:0000:00fb LEN=84 TC=0 HOPLIMIT=255 FLOWLBL=0 PROTO=UDP S
PT=5353 DPT=5353 LEN=44
msctc-linux-spring2014a:/home/preuss #
```

preuss : bash

The presentation shows IPv6 multicast packets being dropped.

preuss : bash - Konsole

1

09:45 AM