Title

Local Privilege Escalation in HP Thin Pro OS

Affected software:

- T6X44017 - ftp://ftp.hp.com/pub/tcdebian/images/T6X44017.dd.gz

- T6X51007 - ftp://ftp.hp.com/pub/tcdebian/images/T6X51007.dd.gz

- T6X52011 - ftp://ftp.hp.com/pub/tcdebian/images/T6X52011.dd.gz

- Z6X52011 - ftp://ftp.hp.com/pub/tcdebian/images/Z6X52011.dd.gz

Credits:

- Roberto Suggi Liverani - @malerisch
- Vincent Hutsebaut - @vhutsebaut

Description/Impact

In HP Thin Pro OS, the sudo configuration allows an unauthenticated user to abuse the keyboard layout tool to perform a privilege escalation attack and gain unauthorised root access on the machine.

The keyboard layout (located in "/usr/bin/hptc-keyboard-layout") runs as a privileged process and it is directly available to an unauthenticated user from the UI (user interface) of the HP Thin Pro Kiosk.

By abusing the available UI controls, an unauthenticated user can navigate on the file system and restore the original /etc/shadow file on the system, which will then allow to set a new admin password on the system.

Conditions

The following conditions are required:

- HP Thin OS Pro set in Kiosk mode;

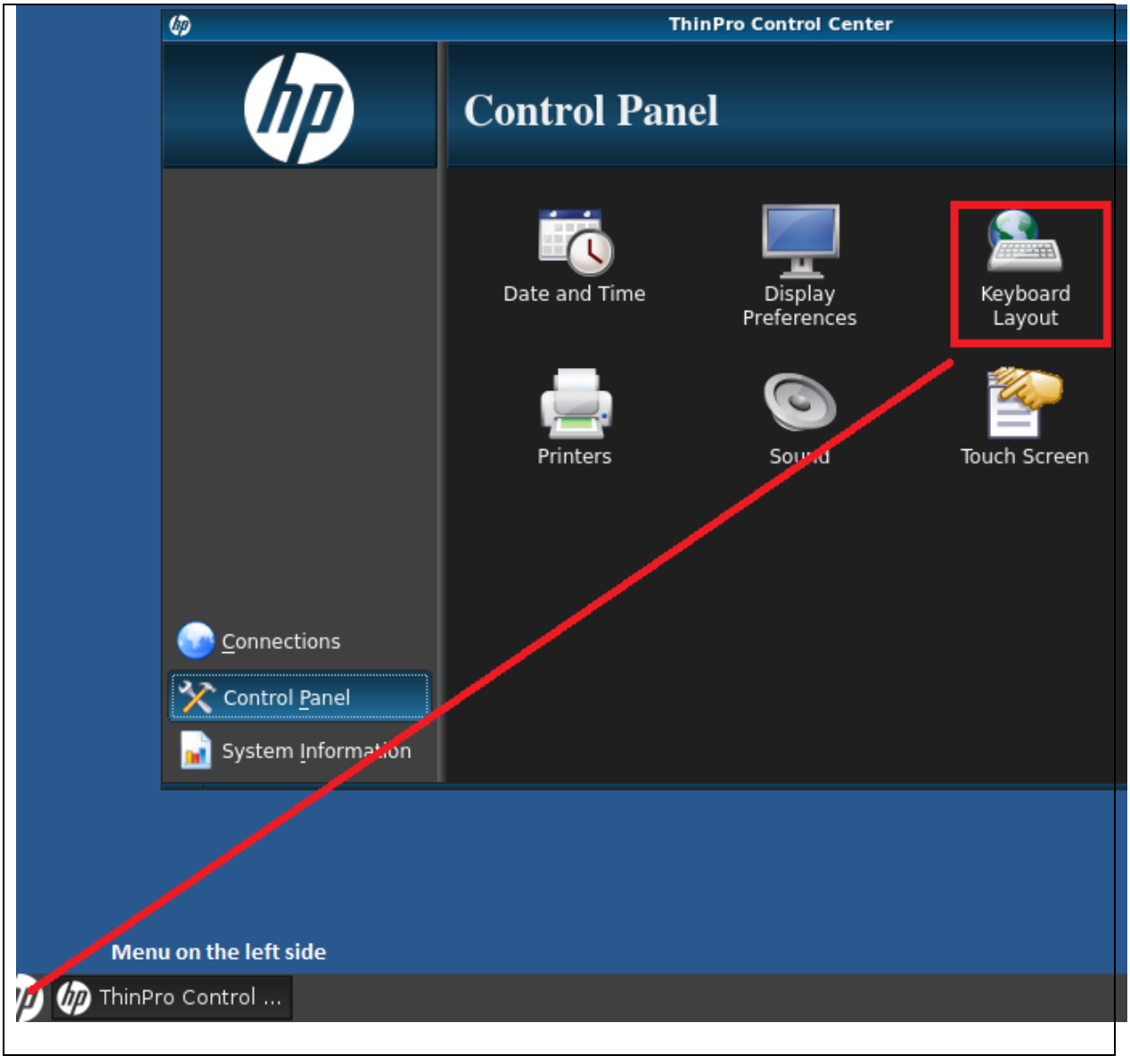
- HP Thin OS Pro - administrator password has already been set by an administrator;

- A malicious user has physical access to the Kiosk but does not have a user account and does not know the admin password.

Steps to reproduce (as a malicious user)

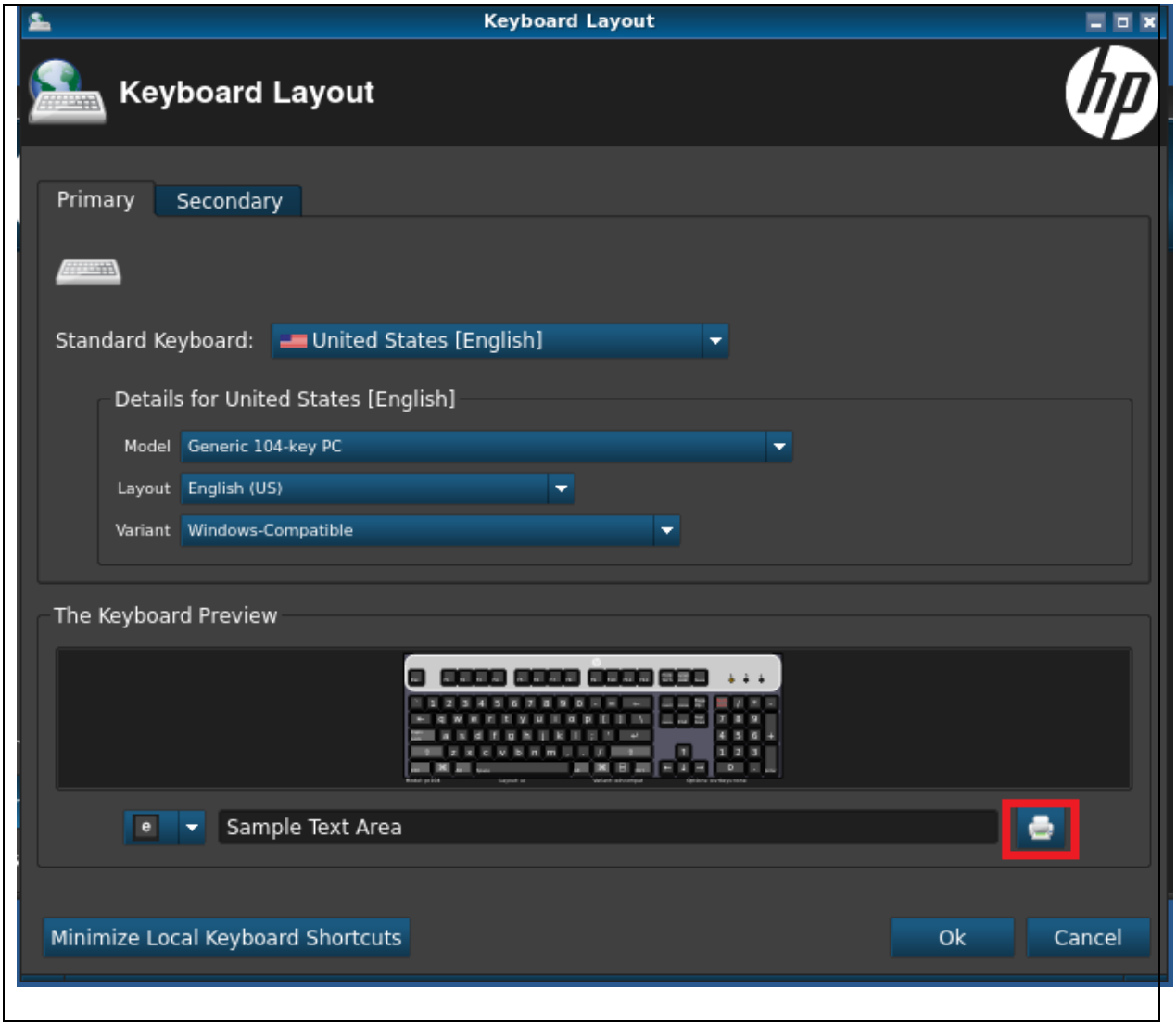
1) Click on the left side, "Control Panel" icon and then clicking the "Keyboard Layout" icon; ** note that the button and UI might be different from the OS version, but the keyboard layout tool is available to an unauthenticated user in Kiosk mode

Step 1 – Figure 1



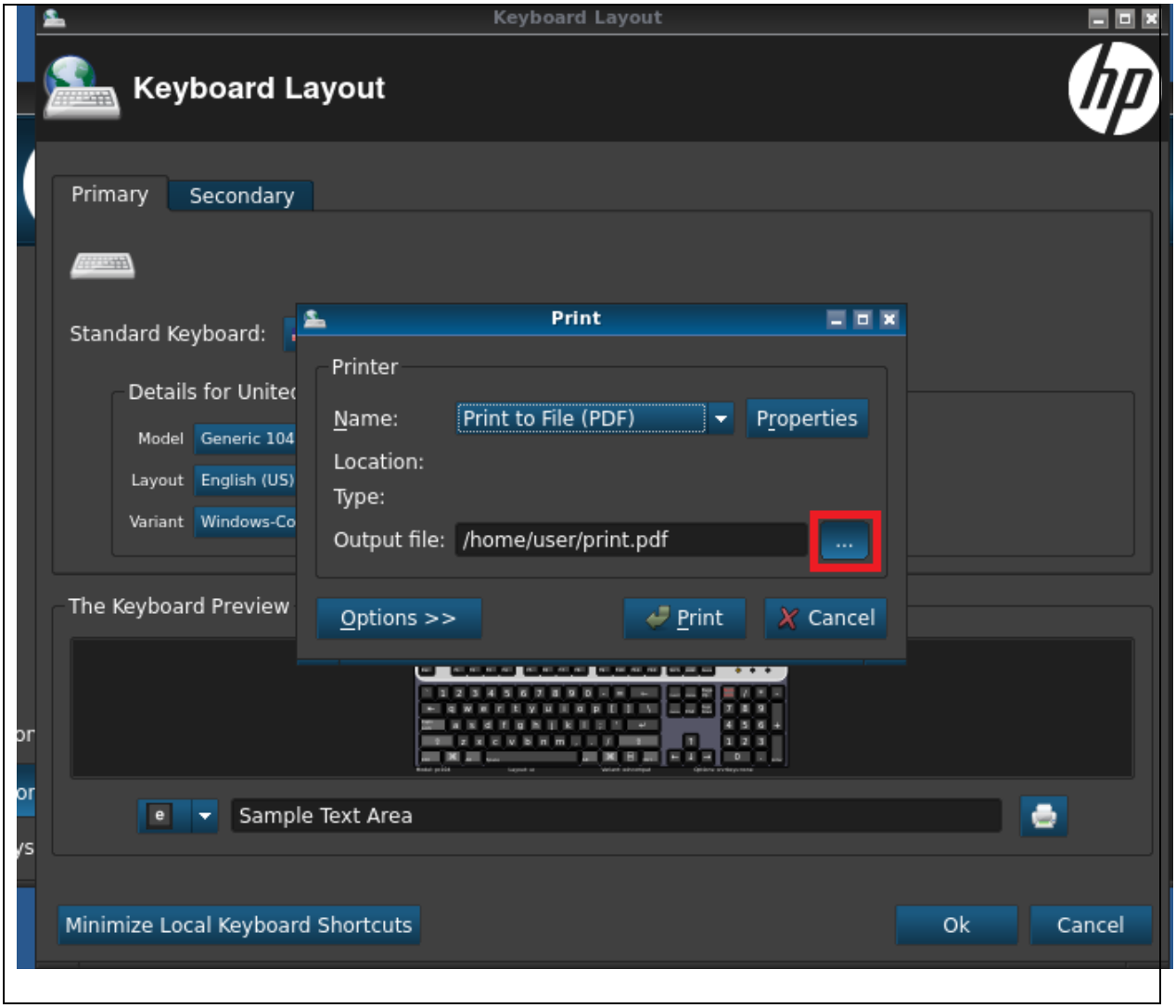
2) Click on print icon, a "Print File" dialog prompt is provided to the user

Step 2 – Figure 1

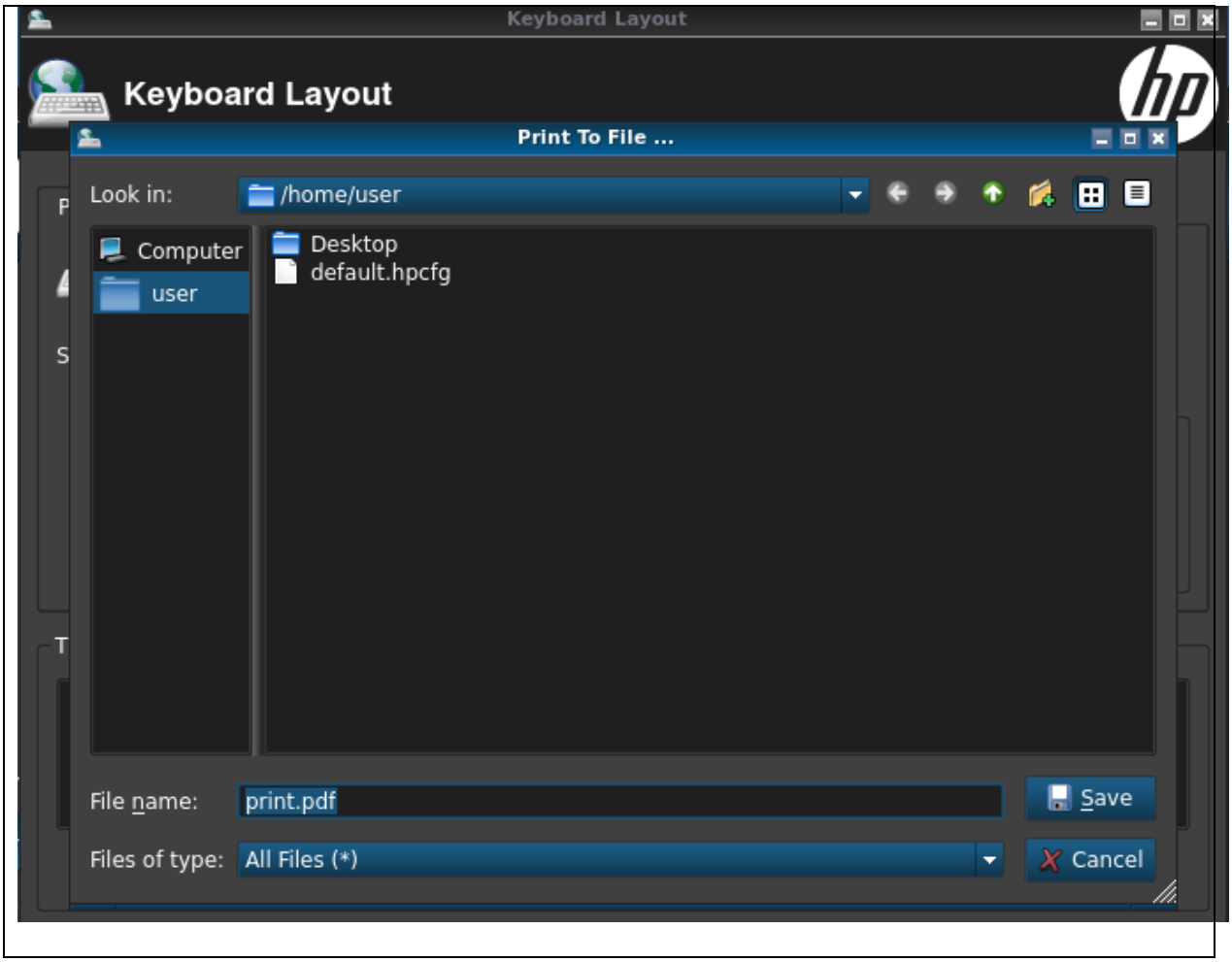


3) Print File dialog allows to set an "output file" - by clicking on the "..." button to choose the folder

Step 3 – Figure 1

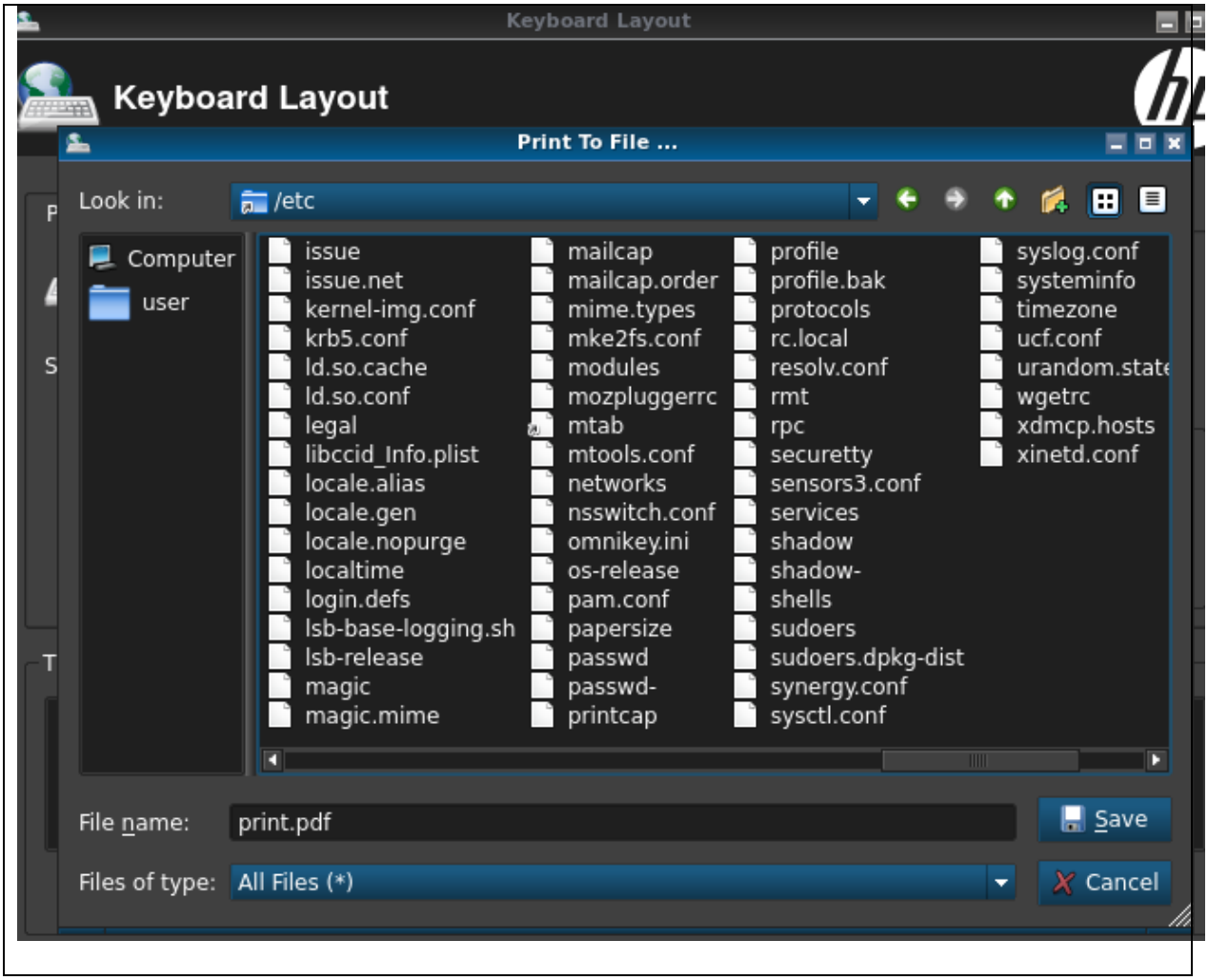


Step 3 – Figure 2



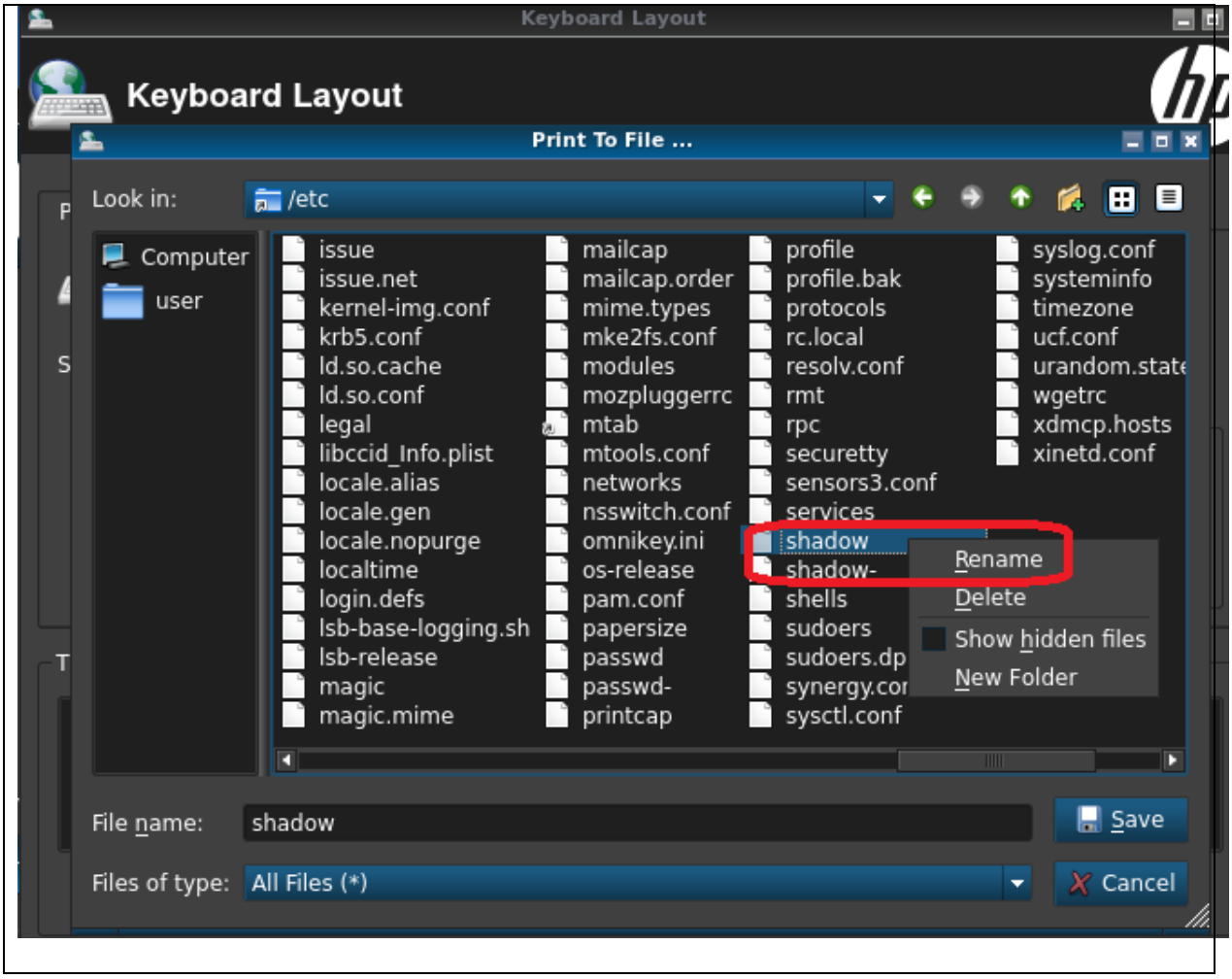
4) Navigate to /etc/ folder

Step 4 – Figure 1

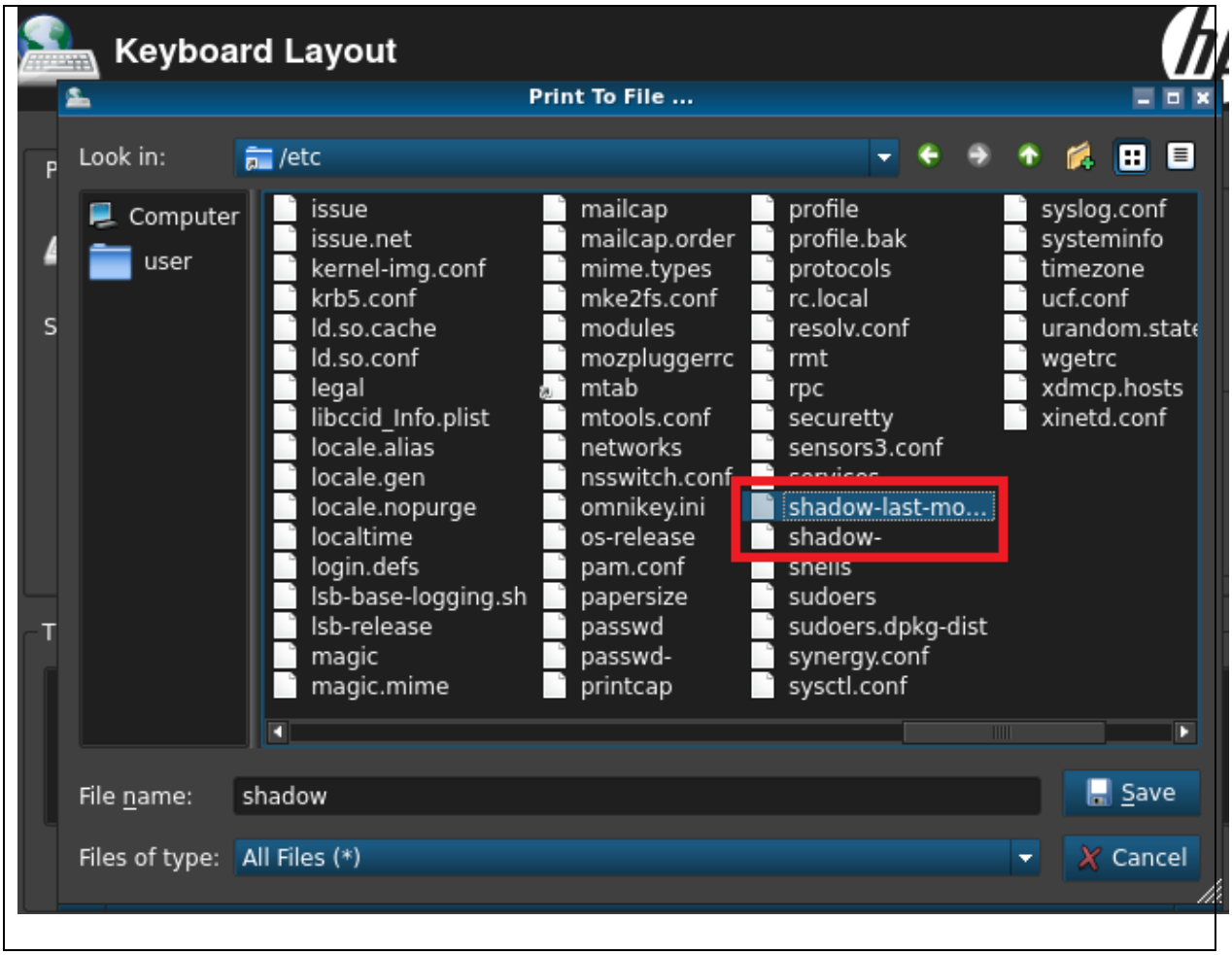


5) Rename /etc/shadow into /etc/shadow-last-modified-by-admin

Step 5 – Figure 1

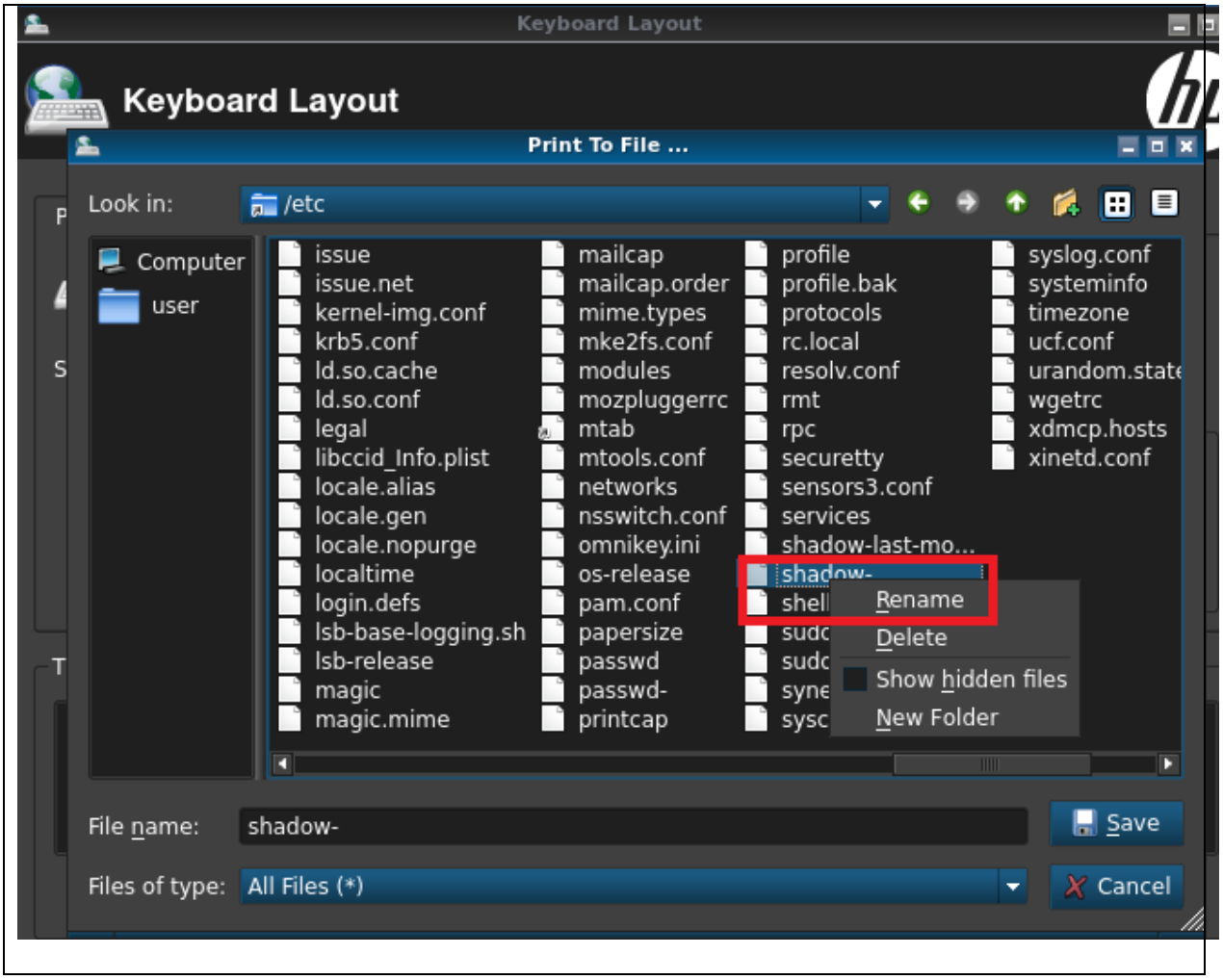


Step 6 – Figure 1


Keyboard Layout
Print To File ...
Look in:
/etc
Computer
user
issue
issue.net
kernel-img.conf
krb5.conf
ld.so.cache
ld.so.conf
legal
libccid_Info.plist
locale.alias
locale.gen
locale.nopurge
localtime
login.defs
lsb-base-logging.sh
lsb-release
magic
magic.mime
mailcap
mailcap.order
mime.types
mke2fs.conf
modules
mozpluggerrc
mtab
mtools.conf
networks
nsswitch.conf
omnikey.ini
os-release
pam.conf
papersize
passwd
passwd-
printcap
profile
profile.bak
protocols
rc.local
resolv.conf
rmt
rpc
securetty
sensors3.conf
shadow-last-mo...
shadow-
sudoers
sudoers.dpkg-dist
synergy.conf
sysctl.conf
syslog.conf
systeminfo
timezone
ucf.conf
urandom.state
wgetrc
xdmcp.hosts
xinetd.conf
File name:
shadow
Save
Files of type:
All Files (*)
Cancel

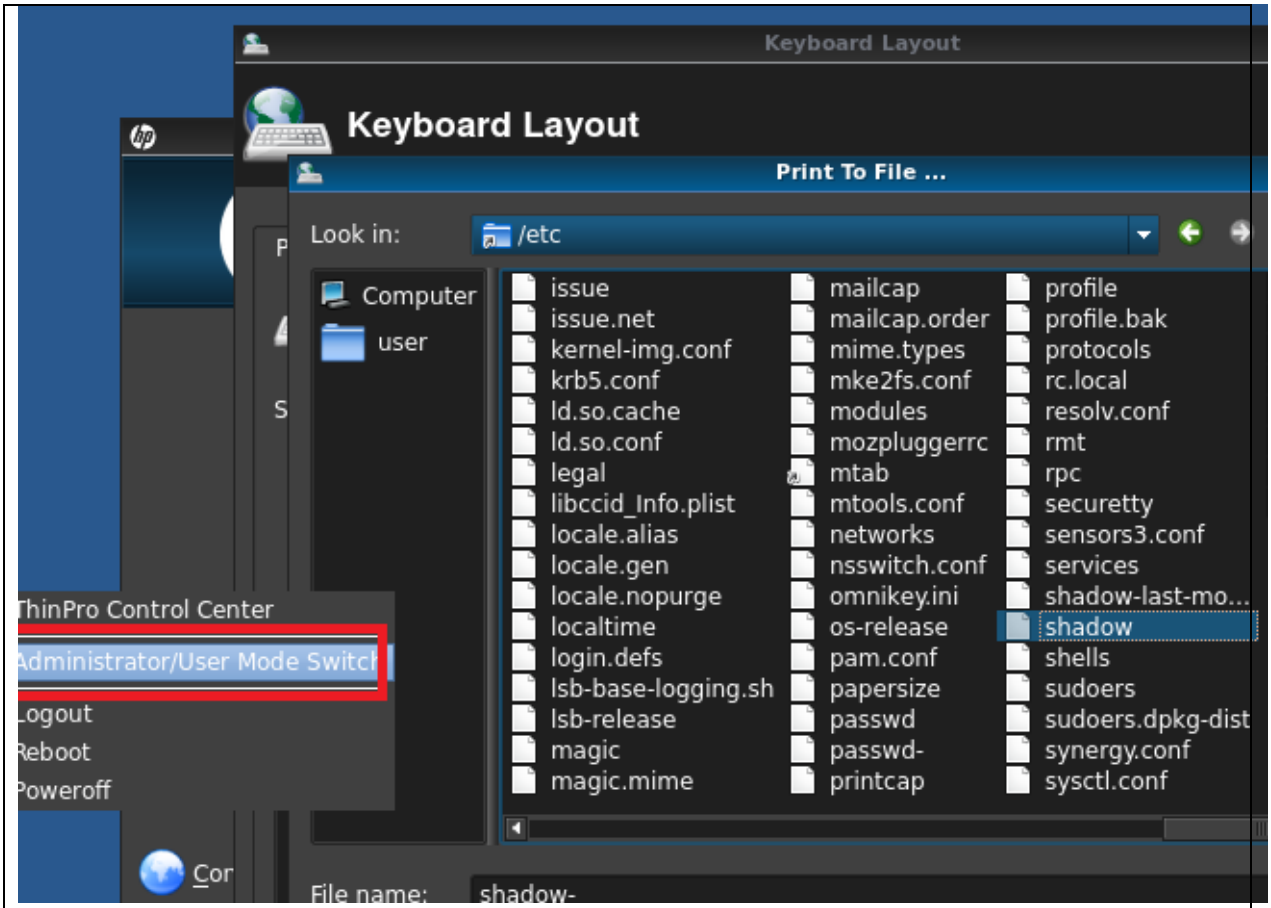
6) Rename /etc/shadow- into /etc/shadow

Step 6 – Figure 1



7) Click on the "Administrator/User Mode Switch"

Step 7 – Figure 1



8) Malicious user can set a new admin password and access the administrator mode of the kiosk

Step 8 – Figure 1

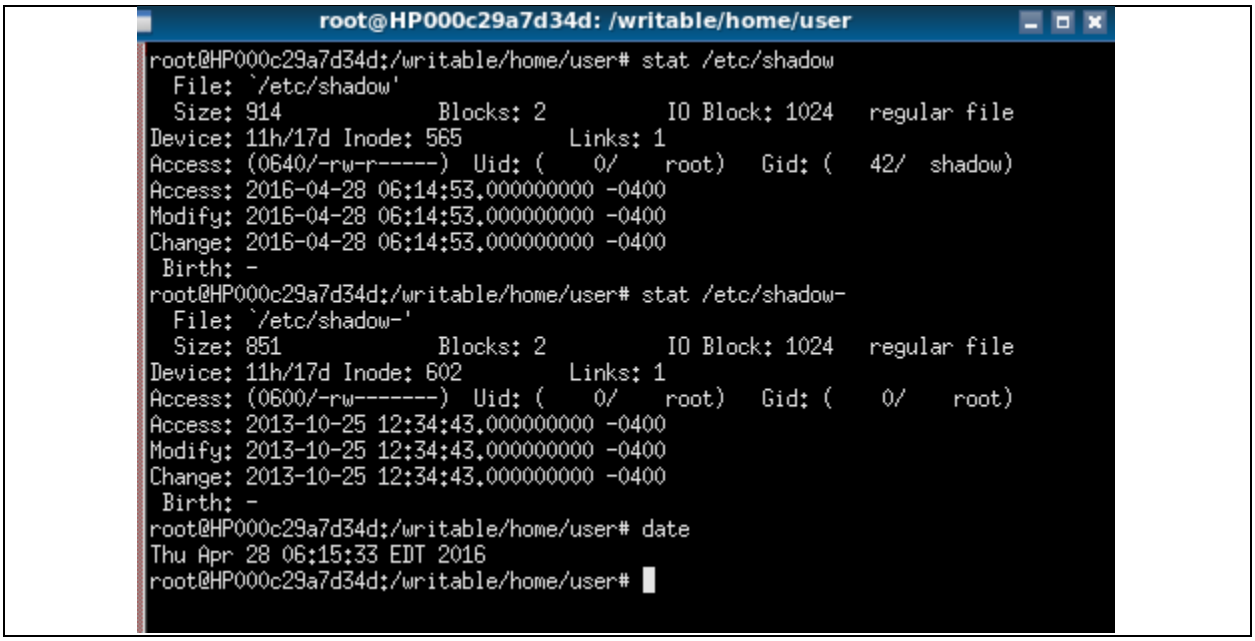
9) Launch an xterminal with root access

Step 9 – Figure 1

Step 9 – Figure 2

Further observations

The /etc/shadow- file remains as the original one even after that the admin password has been changed multiple times. In this example, passwd has already been set twice but the shadow- remains the one set originally in the OS (back in 2013), making the attack described in this report possible:



In the sudoer configuration, it is possible to see the NOPASSWD tag set for the Keyboard Layout tool (usr/bin/hptc-keyboard-layout):