

[About us](#)[Exploits](#)[Learning security](#)[Links](#)[Security tools](#)

You are here : [Home](#) » [Learning security](#) » [Operating Systems](#) » [GNU Linux](#) » VNC to access Kali Linux on Raspberry Pi

VNC to access Kali Linux on Raspberry Pi



30 MAY 2016



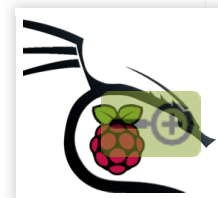
15:24

[EMERIC NASI](#)

6 MESSAGES

License : Copyright Emeric Nasi, some rights reserved

This work is licensed under a [Creative Commons Attribution 4.0 International License](#).



I wrote this how-to because I lastly decided to install and run Kali Linux from a Raspberry Pi. I wanted to install VNC and I found it quite complicated to get the information I needed to be able to do so in a secure and nice way.

I. Prerequisites

First you need to have a running Kali or other Debian based Linux distribution installed on Raspberry Pi. I personally installed Kali 2 on Raspberry Pi 3. For that look at instruction on the [Kali Official Documentation \[http://docs.kali.org/kali-on-arm/install-kali-linux-arm-raspberry-pi\]](http://docs.kali.org/kali-on-arm/install-kali-linux-arm-raspberry-pi)

The device must be connected to the Internet to install the required packages and be network accessible to the PC or phone where you install the VNC client.

SSH server must be available and running on the Raspberry Pi. The Raspberry Pi will act as SSH and VNC server.

I used Xubuntu as the client OS but any other are possible provided they support SSH



tunneling and you can install a VNC client.

Warning: As stated by [Kali Official Documentation \[http://docs.kali.org/kali-on-arm/install-kali-linux-arm-raspberry-pi\]](http://docs.kali.org/kali-on-arm/install-kali-linux-arm-raspberry-pi) all Kali Arm images are configured with the same SSH host key. The host keys must be changed by running:

```
rm /etc/ssh/ssh_host_*  
dpkg-reconfigure openssh-server  
service ssh restart
```

Also you should use certificate authentication for SSH or at least change the default password (toor) for the Kali root user.

II. Install TightVNC

II.1 Required packages

Install TightVNC server package:

```
apt-get install tightvncserver
```

Install Autocutsel package to enable cut&paste between client and server:

```
apt-get install autocutsel
```

II.2 First run

We will make a first run of VncServer to generate configuration files and VNC password.

```
vncserver :1
```

We started an X session on display port 1, note that by default vncserver will attempt to start on display 0 which is already taken by the started Kali session used for local access

The first time you run vncserver, it prompts for a password (8 char max). That's when you realize VNC sessions are not linked to Linux user authentication but relies on a single password (one of VNC insecurity problems)! You can later change that password using the `vncpasswd` command.

We can check the VNCserver is running by issuing the `netstat -tupln` command:



```
tcp      0      0  0.0.0.0:5901      0.0.0.0:*        LISTEN    Xtightvnc
tcp      0      0  0.0.0.0:6001      0.0.0.0:*        LISTEN    Xtightvnc
tcp      0      0  0.0.0.0:22        0.0.0.0:*        LISTEN    sshd
```

Port 5901 is VNC connection port, 6001 is X server for VNC.

II.3 Client access

On the client machine, first install a VNC client such as xtightvncviewer.

```
apt-get install xtightvncviewer
```

To connect to the server use the command:

```
xtightvncviewer <server_ip>:1
```

You may notice that the remote HMI is not responsive and really slow. To remediate to that, you can use some options to optimize the connection:

```
xtightvncviewer <server_ip>:1 -compresslevel 9 -quality 4
-depth 8
```

II.4 Configuration

We will configure VNC startup script to enable cut and paste. For that edit the file `/.vnc/xstartup` and add `autocutsel` line as below.

```
1. #!/bin/sh
2. xrdp $HOME/.Xresources
3. xsetroot -solid grey
4. autocutsel -fork
5. # Fix to make GNOME work
6. export XKL_XMODMAP_DISABLE=1
7. /etc/X11/Xsession
```

You can restart your VNC server and check it is working.

III. VNC over SSH

As mention on TightVNC [man page \[http://www.tightvnc.com/Xvnc.1.php\]](http://www.tightvnc.com/Xvnc.1.php), the problem about Xvnc is that it is not secure. As they write: "It's recommended to restrict network access to Xvnc servers from untrusted network addresses. Probably, the best way to

secure Xvnc server is to allow only loopback connections ... and to use SSH tunneling for remote access to the Xvnc server.”

III.1 Localhost only VNC server

We want all our traffic to go through an SSH tunnel. So we will ensure VNC related ports are not accessible on the network.

We have to start VNC server with next options:

```
vncserver :1 -geometry 1280x800 -depth 16 -localhost -nolisten  
tcp
```

The *-localhost* option will ensure VNC port 5901 is listening only on local interface, the *-nolisten tcp* option will disable the port 6001(X Server will not listen on the network).

Now our listening connections are:

```
tcp      0      0  127.0.0.1:5901    0.0.0.0:*  LISTEN   Xtightvnc  
tcp      0      0  0.0.0.0:22        0.0.0.0:*  LISTEN   sshd
```

III.2 SSH Tunnel

We will create an SSH tunnel by issuing the next command on client machine:

```
ssh -L 5901:localhost:5901 -N -f <distant_user>@<server_ip>
```

This command means SSH will listen on local port 5901 on client machine. Any connection to this port will be tunneled to port 5901 or the remote VNC server via SSH (port 22).

Now to connect to our raspberry pi VNC server we use the command:

```
xtightvncviewer localhost:1 -compresslevel 9 -quality 4 -depth  
8
```

Note: So we have now to enter two passwords, first the distant user password, next the VNC password, it is much more secure. Not sure if that counts as double authentication though :-) !

IV. Enable at boot



IV.1 Startup script

This startup script is an adaptation of the one proposed by [raspberrypi.org](https://www.raspberrypi.org/documentation/remote-access/vnc/README.md) [<https://www.raspberrypi.org/documentation/remote-access/vnc/README.md>] to enable the SSH tunneling.



```
1. #!/bin/sh
2. ### BEGIN INIT INFO
3. # Provides: vncboot
4. # Required-Start: $remote_fs $syslog
5. # Required-Stop: $remote_fs $syslog
6. # Default-Start: 2 3 4 5
7. # Default-Stop: 0 1 6
8. # Short-Description: Start VNC Server at boot time
9. # Description: Start VNC Server at boot time.
10. ### END INIT INFO
11.
12. USER=root
13. HOME=/root
14. export USER HOME
15.
16. case "$1" in
17.     start)
18.         echo "Starting VNC Server"
19.         /usr/bin/vncserver :1 -geometry 1280x800 -depth 16 -local
localhost -nolisten tcp
20.         ;;
21.
22.     stop)
23.         echo "Stopping VNC Server"
24.         /usr/bin/vncserver -kill :1
25.         ;;
26.
27.     *)
28.         echo "Usage: /etc/init.d/vncboot {start|stop}"
29.         exit 1
30.         ;;
31. esac
32.
33. exit 0
```



[Download](#)

You can test this script by issuing `service vncboot start` to start VNC server and `service vncboot stop` to stop it.

IV.2 Enable at startup

To enable the script at machine boot:

```
chmod 755 /etc/init.d/vncboot
update-rc.d vncboot defaults
```

Now enjoy your remote access, and have fun!

Also in this section

20 July 2017 – [Digging passwords in Linux swap](#)

5 December 2010 – [Linux filesystem security scans](#)

27 August 2010 – [Linux security using a limited group \(PAM modules\)](#)

14 August 2010 – [How to secure Linux users](#)

18 June 2010 – [HTTP backdoor using POSIX file capabilities and PHP](#)

6 Forum posts



[VNC to access Kali Linux on Raspberry Pi](#), Bash_Cypher | 29 November 2016 - 08:39



I'm getting a grey screen only. I'm assuming that it's because xstartup

isn't starting a separate xwindow. I'm sure I am doing this right and have tried both /etc/X11/Ssession and /bin/startx /bin/start/xfce ... no luck. Any advice?



VNC to access Kali Linux on Raspberry Pi, Samczar | 30 December 2016 - 23:50

2

I'm getting a grey screen only. I'm assuming that it's because xstartup isn't starting a separate xwindow. I'm sure I am doing this right and have tried both /etc/X11/Ssession and /bin/startx /bin/start/xfce ... no luck. Any advice?



VNC to access Kali Linux on Raspberry Pi, DaveHowe | 6 March 2017 - 13:59

3

I find you often have to specify an xwindows manager in /root/.vnc/xstartup manually when adding vncserver to linux boxes....



VNC to access Kali Linux on Raspberry Pi, Xnehaxixh | 6 October 2017 - 10:19

4

I'm too getting a grey screen. Apparently a solution is posted on this site may help you out:

<https://raspberrypi.stackexchange.com/questions/60874/tightvncserver-displaying-grey-screen-on-kali-linux-upon-vnc-connection> [<https://raspberrypi.stackexchange.com/questions/60874/tightvncserver-displaying-grey-screen-on-kali-linux-upon-vnc-connection>]



VNC to access Kali Linux on Raspberry Pi, Kody | 19 April 2018 - 21:07

5

```
#touch /.Xresources
restart service
```

```
#rm -rf /.Xauthority
restart service
```

This should resolve the grey screen issue.





VNC to access Kali Linux on Raspberry Pi, Radio Pushka | 26 November 2018 - 07:31

6

So I did what you guys told me, and nothing works. all the ports are closed, even the ssh port which usually starts on startup. however, the vnc server does work if started on the command line. The vncboot script not working.

Any message or comments?

