Universidad Oberta De Cataluña

Guía De Aseguramiento Dispositivos Iot: Raspberry PI - Sistema Operativo Raspbian

Yesith Alexander Álvarez Matta

Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions.

TFM-Sandbox environment for IoT malware.

Junio, 2020

Contenido

1. Introducción

Este documento contiene información de configuración segura sobre el sistema operativo Raspbian diseñado para la Raspberry PI, en sus versiones 4.19.97 y anteriores. Esta configuración deberá ser evaluada por un personal capacitado de tecnología antes de proceder a su implementación en un ambiente productivo, ya que puede impactar el funcionamiento de las soluciones, aplicaciones o servicios sobre este sistema operativo.

2. Objetivo

El objetivo de este documento es presentar los procedimientos de configuración de línea base de seguridad para el sistema operativo Raspbian diseñado para la Raspberry PI.

3. Recomendaciones de Seguridad

Los procedimientos definidos en esta guía de aseguramiento deben ser probados, validados y confirmados en ambientes de laboratorio antes de su implementación en un ambiente productivo, ya que estas configuraciones pueden impactar el correcto funcionamiento las aplicaciones, funcionalidades o servicios, llegando a implicar una reinstalación o configuración adicional sobre el sistema operativo de la raspberry.

Cabe aclarar que antes de implementar cualquier procedimiento de esta guía se debe realizar un respaldo completo del sistema, la información y los aplicativos que se utilicen.

4. Cambio de Credenciales por defecto.

Una vez instalado el sistema operativo del dispositivo realice un cambio de usuario y de contraseña de manera inmediata, evitando contraseñas que se relacionen con el dispositivo y que sean fáciles de adivinar. Procure el uso de mayúsculas minúsculas, números y caracteres especiales con un tamaño mínimo de 16 Dígitos.

Cambio de contraseña:

```
# passwd
```

5. Actualizaciones de Software

Con frecuencia raspberrypi.org lanza actualizaciones de sistema operativo con el fin de ofrecer nuevas funcionalidades y corregir fallos de seguridad, asegúrese de instalar con frecuencia las actualizaciones, parches y software de seguridad adicional.

Actualización de repositorios y directorios:

```
# apt-get update
```

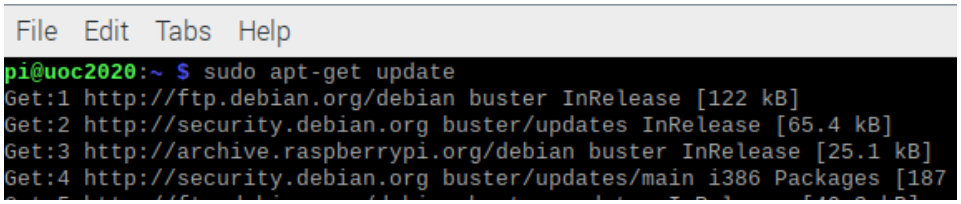

Imagen 1. Actualización de Directorios para actualización.

Actualización de sistema Operativo:

```
# apt-get upgrade
```

```
File  Edit  Tabs  Help
pi@uoc2020:~ $ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no long
  gstreamer0.10-alsa gstreamer0.10-plugins-base libgstreamer-plugin
libgstreamer0.10-0 libxfce4util-bin libxfce4util-common libxfce4uti
```

Imagen 2. Actualización de Sistema Operativo.

Verificación: Verifique que no haya actualizaciones o parches para instalar.

 # apt-get -s upgrade

```
pi@uoc2020:~ $ sudo apt-get -s  upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  gstreamer0.10-alsa gstreamer0.10-plugins-base
  libgstreamer-plugins-base0.10-0 libgstreamer0.10-0 libxfce4util-bin
  libxfce4util-common libxfce4util7 libxfconf-0-2 multiarch-support pimixer
  point-rpi xfconf
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  libjavascriptcoregtk-4.0-18 libwebkit2gtk-4.0-37 linux-headers-amd64:amd64
  linux-image-amd64:amd64 raspberrypi-sys-mods
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
```

Imagen 3. Verificación de parches y actualizaciones.

6. Servicios de sistema Operativo

Telnet:

- Deshabilite el servicio telnet (Telnet-Server): El protocolo telnet es inseguro y no transmite la información cifrada, en su lugar utilice el servicio SSH.

- Deshabilite el servicio telnet (Telnet-Client): El protocolo telnet es inseguro y no transmite la información cifrada, en su lugar utilice el servicio SSH.

Desinstalación:

```
# apt purge telnet
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
#  dpkg -s telnet
```

```
pi@uoc2020:~ $ sudo dpkg -s telnet
dpkg-query: package 'telnet' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

Imagen 4. Verificación de Software instalado.

RSH:

- Deshabilite el servicio rsh (RSH-Server): Este servicio transmite credenciales o passwords en texto plano por lo tanto se debe deshabilitar, en su lugar utilice el servicio SSH.

Desinstalación:

```
# apt purge rsh-client
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# dpkg -s rsh-client
```

```
pi@uoc2020:~ $ sudo dpkg -s rsh-client
dpkg-query: package 'rsh-client' is not installed and no information is availabl
e
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

Imagen 5. Verificación de Software instalado.

- Deshabilite el servicio rsh (RSH-Client): Este servicio transmite credenciales o passwords en texto plano por lo tanto se debe deshabilitar, en su lugar utilice el servicio SSH.

Desinstalación:

```
# apt purge rsh-server
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# dpkg -s rsh-server
```

```
pi@uoc2020:~ $ sudo dpkg -s rsh-server
dpkg-query: package 'rsh-server' is not installed and no information is availabl
e
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

Imagen 6. Verificación de Software instalado.

TFTP:

- Deshabilite el servicio TFTP (TFTP-Server): TFTP no admite autenticación, se debe deshabilitar.

Desinstalación:

```
# apt purge tftp
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# dpkg -s tftp
```

```
pi@uoc2020:~ $ sudo dpkg -s tftp
dpkg-query: package 'tftp' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

Imagen 7. Verificación de Software instalado.

Talk:

- Deshabilite el servicio talk (Talk-Server): Este servicio no utiliza protocolos de cifrados para su comunicación por lo cual la información transmitida corre riesgo de ser capturada y se debe deshabilitar.

Desinstalación:

```
# apt purge tftp
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# dpkg -s tftp
```

```
pi@uoc2020:~ $ sudo dpkg -s tftp
dpkg-query: package 'tftp' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

Imagen 8. Verificación de Software instalado.

NIS:

- Deshabilite el servicio NIS (NIS-Server): Este servicio es vulnerable a ataques de denegación de servicio. Se debe deshabilitar

Desinstalación:

```
# systemctl --now disable nis
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled nis
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled nis
Failed to get unit file state for nis.service: No such file or directory
```

Imagen 9. Verificación de Software instalado.

- Deshabilite el servicio NIS (NIS-Client): Este servicio es vulnerable a ataques de denegación de servicio. Se debe deshabilitar

Desinstalación:

```
# apt purge nis
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# dpkg -s nis
```

```
pi@uoc2020:~ $ sudo dpkg -s nis
dpkg-query: package 'nis' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

Imagen 10. Verificación de Software instalado

7. Servicios de sistema Operativo con propósito

DHCP:

- Deshabilite el servicio DHCP: A menos que el dispositivo se especifique para prestar un servicio DHCP, se debe deshabilitar este servicio.

Desinstalación:

```
# systemctl --now disable isc-dhcp-server
# systemctl --now disable isc-dhcp-server6
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled isc-dhcp-server
# systemctl is-enabled isc-dhcp-server6
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled isc-dhcp-server
Failed to get unit file state for isc-dhcp-server.service: No such file or direc
tory
pi@uoc2020:~ $ sudo systemctl is-enabled isc-dhcp-server6
Failed to get unit file state for isc-dhcp-server6.service: No such file or dire
ctory
```

Imagen 11. Verificación de Software instalado.

LDAP:

- Deshabilite el servicio LDAP: A menos que el dispositivo se especifique para prestar un servicio de LDAP, se debe deshabilitar este servicio.

Desinstalación:

```
# systemctl --now disable slapd
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled slapd
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled slapd
Failed to get unit file state for slapd.service: No such file or directory
```

Imagen 12. Verificación de Software instalado.

DNS:

- Deshabilite el servicio DNS: A menos que el dispositivo se especifique para prestar un servicio de DNS, se debe deshabilitar este servicio.

Desinstalación:

```
# systemctl --now disable bind9
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled bind9
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled bind9
Failed to get unit file state for bind9.service: No such file or directory
```

Imagen 13. Verificación de Software instalado.

FTP:

- Deshabilite el servicio FTP: Este servicio transmite credenciales o passwords en texto plano por lo tanto se debe deshabilitar, en su lugar utilice el servicio SFTP.

Desinstalación:

```
# systemctl --now disable vsftpd
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled vsftpd
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled vsftpd
Failed to get unit file state for vsftpd.service: No such file or directory
```

Imagen 14. Verificación de Software instalado.

HTTP:

- Deshabilite el servicio HTTP (HTTP-Server): Este servicio transmite credenciales o passwords en texto plano por lo tanto se debe deshabilitar, en su lugar utilice el servicio HTTPS.

Desinstalación:

```
# systemctl --now disable apache2
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled apache2
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled apache2
Failed to get unit file state for apache2.service: No such file or directory
```

Imagen 15. Verificación de Software instalado.

IMAP POP3:

- Deshabilite el servicio IMAP POP3: A menos que el dispositivo se especifique para prestar un servicio de IMAP POP3, se debe deshabilitar este servicio.

Desinstalación:

```
# systemctl --now disable dovecot
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled dovecot
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled dovecot
Failed to get unit file state for dovecot.service: No such file or directory
```

Imagen 16. Verificación de Software instalado.

Samba:

- Deshabilite el servicio Samba: A menos que el dispositivo se especifique para prestar un servicio de Samba para sistemas Windows, se debe deshabilitar este servicio.

Desinstalación:

```
# systemctl --now disable smbd
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled smbd
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled smbd
Failed to get unit file state for smbd.service: No such file or directory
```

Imagen 17. Verificación de Software instalado.

HTTP Proxy:

- Deshabilite el servicio HTTP Proxy: A menos que el dispositivo se especifique para prestar un servicio de HTTP Proxy, se debe deshabilitar este servicio.

Desinstalación:

```
# systemctl --now disable squid
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled squid
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled squid
Failed to get unit file state for squid.service: No such file or directory
```

Imagen 18. Verificación de Software instalado

SNMP:

- Deshabilite el servicio SNMP: A menos que el dispositivo se especifique para prestar un servicio de SNMP, se debe deshabilitar este servicio.

Desinstalación:

```
# systemctl --now disable snmpd
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# systemctl is-enabled snmpd
```

```
pi@uoc2020:~ $ sudo systemctl is-enabled snmpd
Failed to get unit file state for snmpd.service: No such file or directory
```

Imagen 19. Verificación de Software instalado

8. Configuraciones de red

Como regla general sobre cualquier aseguramiento de un sistema informático y con el fin de reducir los posibles ataques al dispositivo, todos los protocolos, aplicaciones, servicios y dispositivos de red no utilizados deben ser deshabilitados de manera permanente con el fin de mitigar cualquier espacio por parte de un atacante o un malware especializado.

IP Forwarding:

- Este servicio es usado para el reenvió de paquetes. Si el servidor no es usado como router se debe deshabilitar.

Desinstalación:

```
# grep -Els "^\s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri "s/^\s*(net\.ipv4\.ip_forward\s*)(=)(\s*\S+\b).*$/# *REMOVED* \1/" $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl –w net.ipv4.route.flush=1
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# sysctl net.ipv4.ip_forward
# sysctl net.ipv4.ip_forward
```

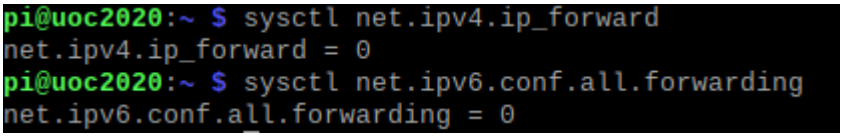

Imagen 20. Verificación de Funcionalidad.

Deshabilite IPv6:

- Deshabilite el protocolo IPv6, a menos que el dispositivo se encuentre en una configuración de red sobre este protocolo.

Desinstalación: Modifique el archivo grub en la siguiente ruta:

```
# nano /etc/default/grub
```

```
pi@uoc2020:~ $ sudo nano /etc/default/grub
```

Imagen 21. Abriendo archivo grub.

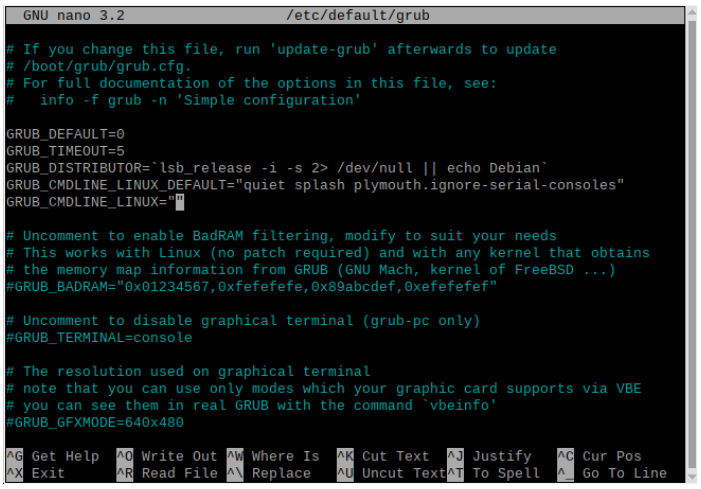

Imagen 22. Archivo grub abierto.

```
# GRUB_CMDLINE_LINUX="ipv6.disable=1"
```

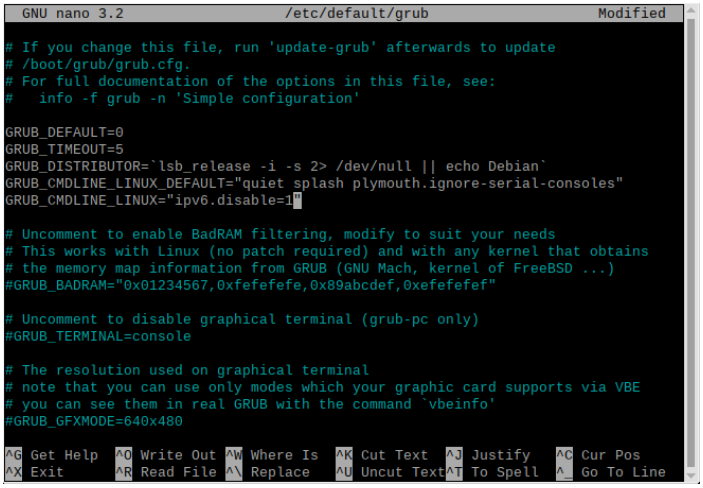

Imagen 23. Modificación de parámetro.

```
# update-grub
```

```
pi@uoc2020:~ $ sudo update-grub
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-4.19.0-6-amd64
Found initrd image: /boot/initrd.img-4.19.0-6-amd64
done
```

Imagen 24. Actualización de grub.

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "ipv6.disable=1"
```

O utilice ifconfig para validar si tiene IPv6 asignada:

```
pi@uoc2020:~ $ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:9a:88:f2  txqueuelen 1000  (Ethernet)
        RX packets 612548  bytes 913376050 (871.0 MiB)
        RX errors 2337  dropped 0  overruns 0  frame 0
        TX packets 296884  bytes 16160459 (15.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000
```

Interfaces inalámbricas (Wireless):

- Deshabilite la interfaz de Wireless, a menos que el dispositivo se especifique para prestar este servicio:

Desinstalación:

```
# nmcli radio all off
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# raspi-config
```

Imagen 25. Verificación de Funcionalidad.

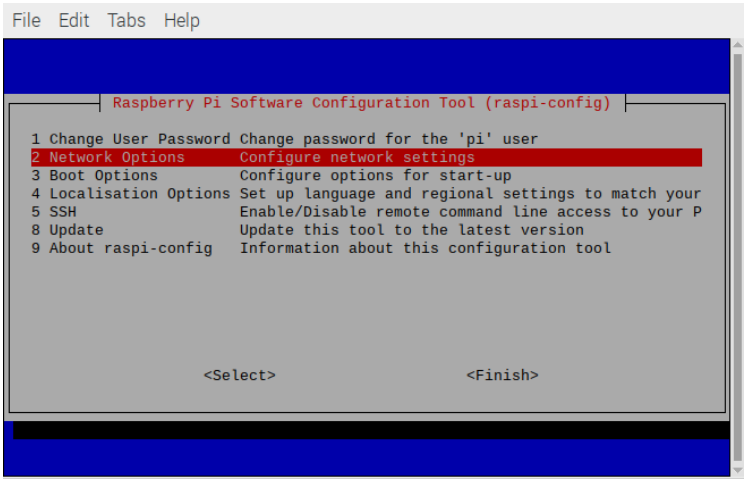

Imagen 26. Menú de configuración.

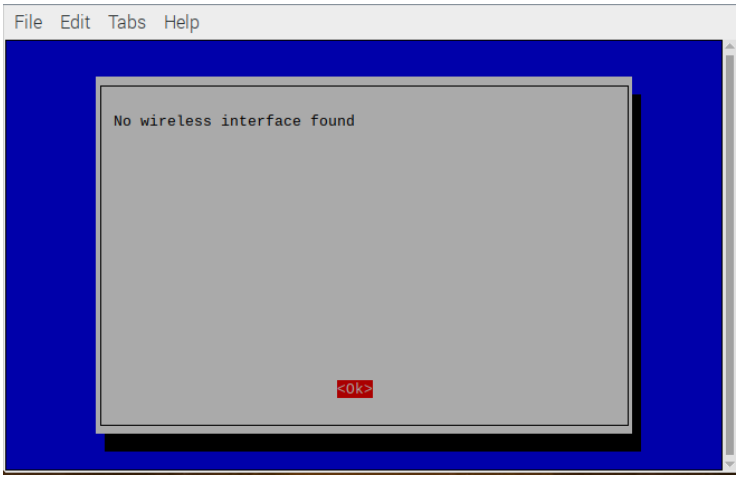

Imagen 27. Verificación de Funcionalidad.

9. Configuración de Servicio SSH

- Deshabilite el servicio SSH: A menos que el dispositivo se especifique para prestar un servicio de SSH, se debe deshabilitar este servicio.

Desinstalación:

```
# nmcli radio all off
```

Verificación: Para auditoria o verificación utilice el siguiente comando.

```
# raspi-config
```

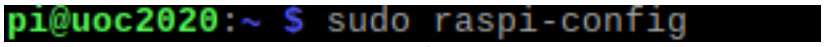

Imagen 28. Verificación de Funcionalidad.

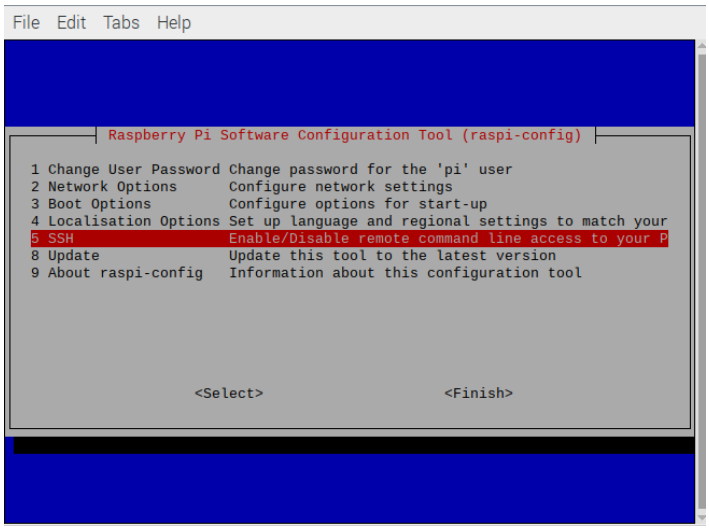

Imagen 29. Menú de configuración.

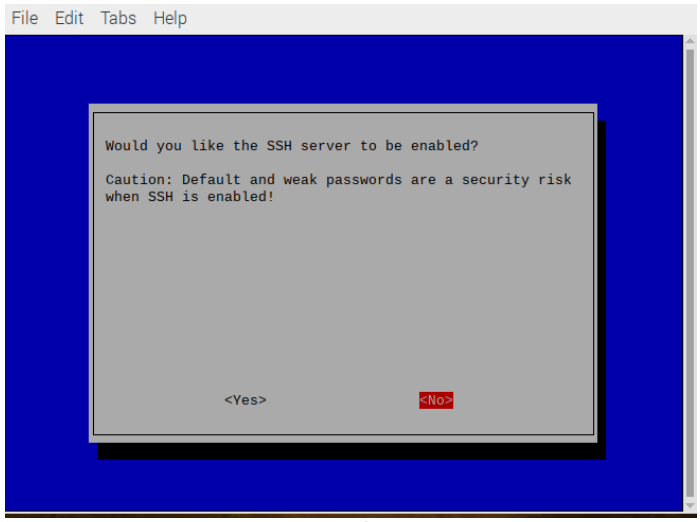

Imagen 30. Verificación de Funcionalidad.

- Si es imprescindible el uso SSH, realice las siguientes configuraciones con el fin de minimizar el riesgo:

  Habilite el servicio con el procedimiento anterior:

Imagen 31.

10. Bibliografía y Referencias

- **Securing your Raspberry:** https://www.raspberrypi.org/documentation/configuration/security.md
- **CIS Benchmark:** https://www.cisecurity.org/cybersecurity-best-practices/
- **CIS Benchmark:** CIS_Debian_Linux_10_Benchmark_v1.0.0.pdf
- **CIS Benchmark:** CIS_Debian_Linux_10_Benchmark_v1.0.0.pdf