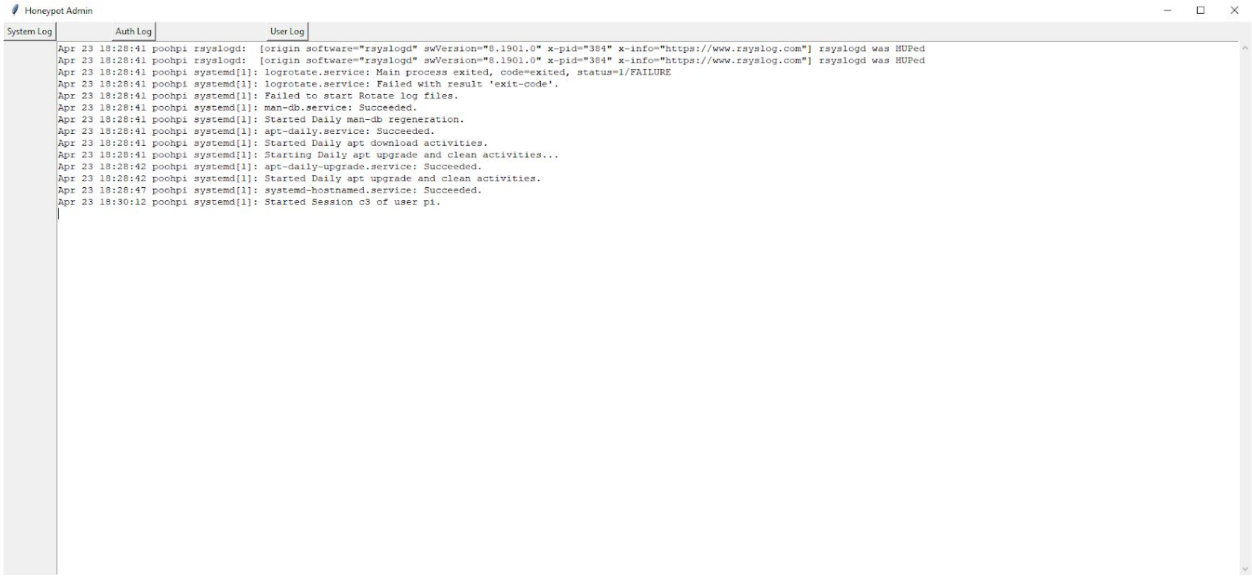
Malicious Honeypot User Manual

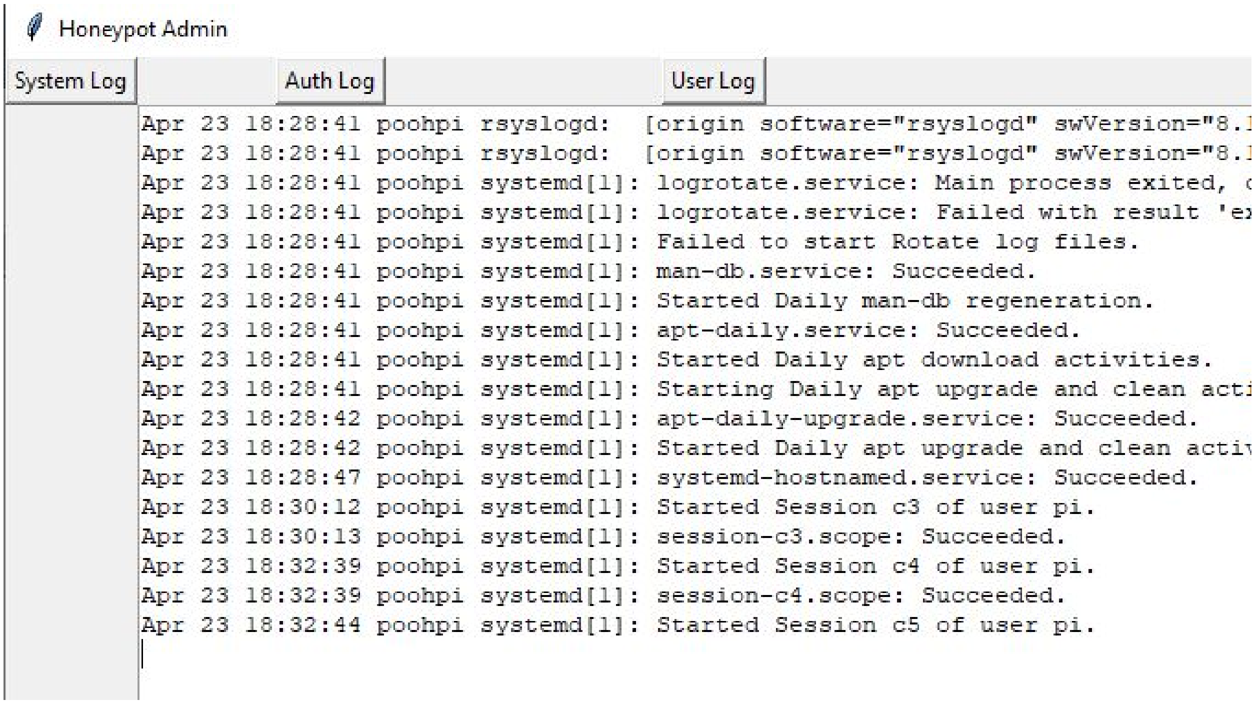
Honeypot Admin Console

The Honeypot Admin console is used for observing a few different log files that are written on the server. There are 3 buttons to load a respective log file. The Console reads a log file from the server and writes a new log file on the admin machine. The log files are organized by date. *(This has only been tested on Windows 10)



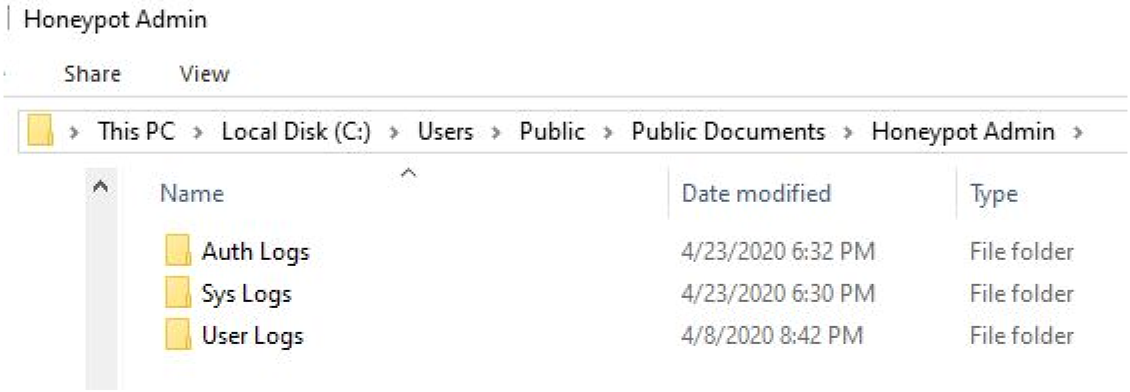
```
Apr 23 18:28:41 poohpi rsyslogd:  [origin software="rsyslogd" swVersion="8.1901.0" x-pid="384" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
Apr 23 18:28:41 poohpi rsyslogd:  [origin software="rsyslogd" swVersion="8.1901.0" x-pid="384" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
Apr 23 18:28:41 poohpi systemd[1]: logrotate.service: Main process exited, code=exited, status=1/FAILURE
Apr 23 18:28:41 poohpi systemd[1]: logrotate.service: Failed with result 'exit-code'.
Apr 23 18:28:41 poohpi systemd[1]: Failed to start Rotate log files.
Apr 23 18:28:41 poohpi systemd[1]: man-db.service: Succeeded.
Apr 23 18:28:41 poohpi systemd[1]: Started Daily man-db regeneration.
Apr 23 18:28:41 poohpi systemd[1]: apt-daily.service: Succeeded.
Apr 23 18:28:41 poohpi systemd[1]: Started Daily apt download activities.
Apr 23 18:28:41 poohpi systemd[1]: Starting Daily apt upgrade and clean activities...
Apr 23 18:28:42 poohpi systemd[1]: apt-daily-upgrade.service: Succeeded.
Apr 23 18:28:42 poohpi systemd[1]: Started Daily apt upgrade and clean activities.
Apr 23 18:28:47 poohpi systemd[1]: systemd-hostnamed.service: Succeeded.
Apr 23 18:30:12 poohpi systemd[1]: Started Session c3 of user pi.
```

Closer look at Honeypot Admin Console



```
Apr 23 18:28:41 poohpi rsyslogd:  [origin software="rsyslogd" swVersion="8.1
Apr 23 18:28:41 poohpi rsyslogd:  [origin software="rsyslogd" swVersion="8.1
Apr 23 18:28:41 poohpi systemd[1]: logrotate.service: Main process exited, c
Apr 23 18:28:41 poohpi systemd[1]: logrotate.service: Failed with result 'ex
Apr 23 18:28:41 poohpi systemd[1]: Failed to start Rotate log files.
Apr 23 18:28:41 poohpi systemd[1]: man-db.service: Succeeded.
Apr 23 18:28:41 poohpi systemd[1]: Started Daily man-db regeneration.
Apr 23 18:28:41 poohpi systemd[1]: apt-daily.service: Succeeded.
Apr 23 18:28:41 poohpi systemd[1]: Started Daily apt download activities.
Apr 23 18:28:41 poohpi systemd[1]: Starting Daily apt upgrade and clean acti
Apr 23 18:28:42 poohpi systemd[1]: apt-daily-upgrade.service: Succeeded.
Apr 23 18:28:42 poohpi systemd[1]: Started Daily apt upgrade and clean activ
Apr 23 18:28:47 poohpi systemd[1]: systemd-hostnamed.service: Succeeded.
Apr 23 18:30:12 poohpi systemd[1]: Started Session c3 of user pi.
Apr 23 18:30:13 poohpi systemd[1]: session-c3.scope: Succeeded.
Apr 23 18:32:39 poohpi systemd[1]: Started Session c4 of user pi.
Apr 23 18:32:39 poohpi systemd[1]: session-c4.scope: Succeeded.
Apr 23 18:32:44 poohpi systemd[1]: Started Session c5 of user pi.
```

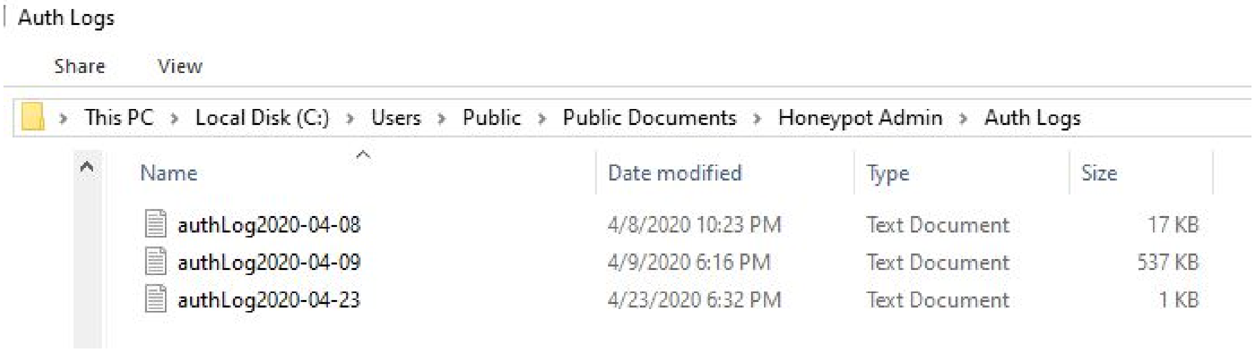
Log Files



Honeypot Admin

This PC › Local Disk (C:) › Users › Public › Public Documents › Honeypot Admin ›

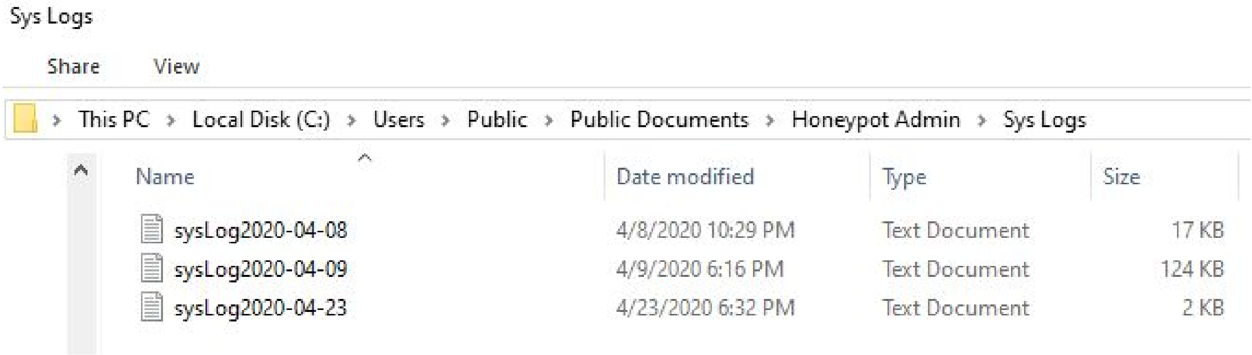
Name	Date modified	Type
Auth Logs	4/23/2020 6:32 PM	File folder
Sys Logs	4/23/2020 6:30 PM	File folder
User Logs	4/8/2020 8:42 PM	File folder



Auth Logs

This PC › Local Disk (C:) › Users › Public › Public Documents › Honeypot Admin › Auth Logs

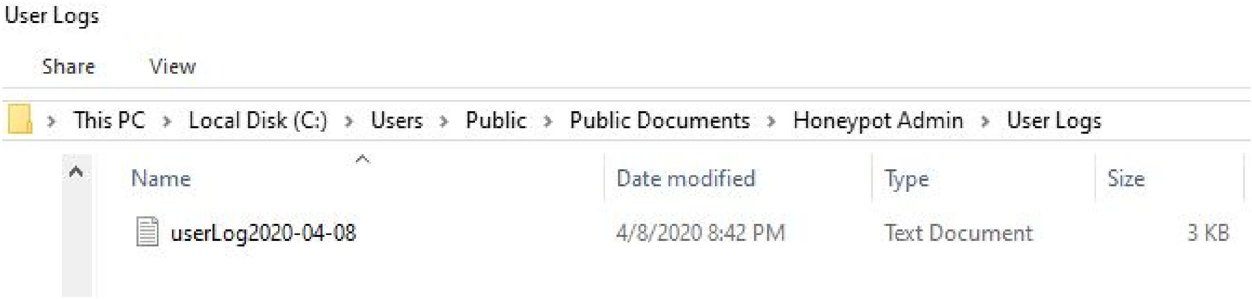
Name	Date modified	Type	Size
authLog2020-04-08	4/8/2020 10:23 PM	Text Document	17 KB
authLog2020-04-09	4/9/2020 6:16 PM	Text Document	537 KB
authLog2020-04-23	4/23/2020 6:32 PM	Text Document	1 KB



Sys Logs

This PC › Local Disk (C:) › Users › Public › Public Documents › Honeypot Admin › Sys Logs

Name	Date modified	Type	Size
sysLog2020-04-08	4/8/2020 10:29 PM	Text Document	17 KB
sysLog2020-04-09	4/9/2020 6:16 PM	Text Document	124 KB
sysLog2020-04-23	4/23/2020 6:32 PM	Text Document	2 KB



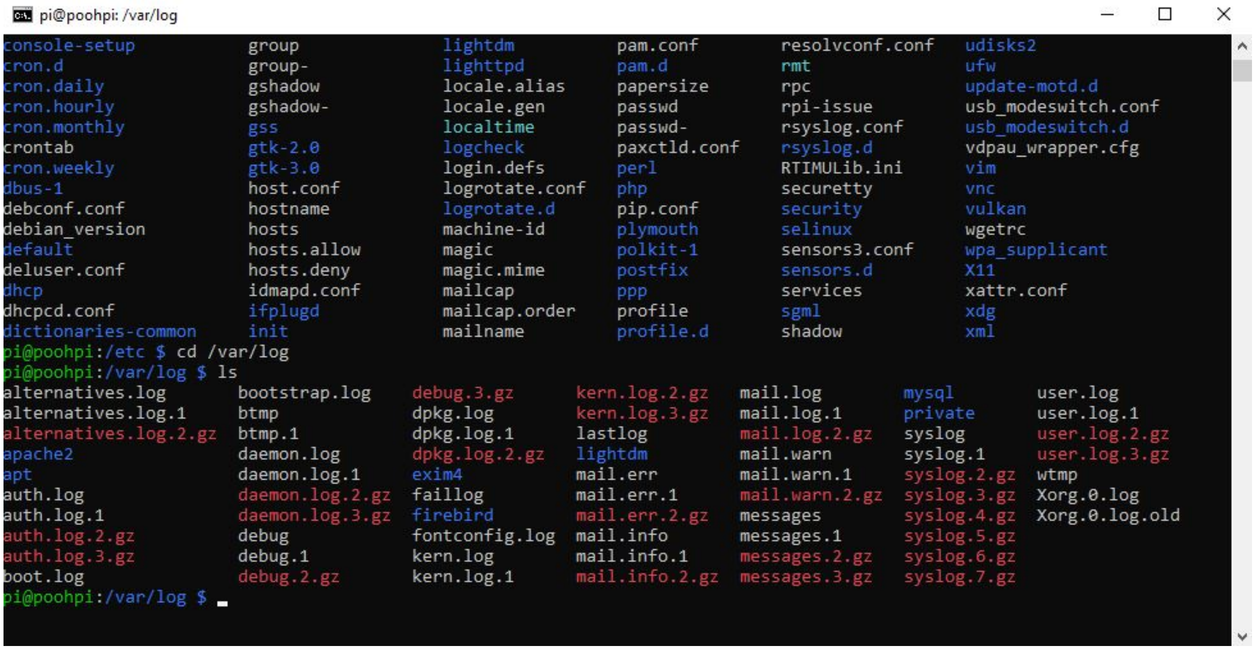
User Logs

This PC › Local Disk (C:) › Users › Public › Public Documents › Honeypot Admin › User Logs

Name	Date modified	Type	Size
userLog2020-04-08	4/8/2020 8:42 PM	Text Document	3 KB

The Honeypot

The Honeypot was hosted on a Raspberry Pi running a Linux based operating system (Raspbian). Ultimately, there would be little to no need to log into the server once all or most of the desired features are automated, but this is where a lot of the work and set up took place on this project. Navigate the directories using cd and ls. Use “Vim” to edit files by typing “vi [filename].” (see vim guide linked below for more commands) Install services like “mailutils” and “WordPress” using “apt-get.”
[“Basic Vim commands - For getting started”]:
https://coderwall.com/p/adv71w/basic-vim-commands-for-getting-started

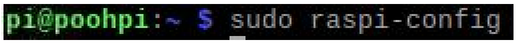


```
console-setup           group              lightdm          pam.conf        resolvconf.conf   udisks2
cron.d                  group-             lighttpd         pam.d           rmt               ufw
cron.daily              gshadow            locale.alias     papersize       rpc               update-motd.d
cron.hourly             gshadow-           locale.gen       passwd          rpi-issue         usb_modeswitch.conf
cron.monthly            gss                localtime        passwd-         rsyslog.conf      usb_modeswitch.d
crontab                 gtk-2.0            logcheck         paxctld.conf    rsyslog.d         vdpau_wrapper.cfg
cron.weekly             gtk-3.0            login.defs       perl            RTIMULib.ini      vim
dbus-1                  host.conf          logrotate.conf   php             securetty         vnc
debconf.conf            hostname           logrotate.d      pip.conf        security          vulkan
debian_version          hosts              machine-id       plymouth        selinux           wgetrc
default                 hosts.allow        magic            polkit-1        sensors3.conf     wpa_supplicant
deluser.conf            hosts.deny         magic.mime       postfix         sensors.d         X11
dhcp                    idmapd.conf        mailcap          ppp             services          xattr.conf
dhcpcd.conf             ifplugd            mailcap.order    profile         sgml              xdg
dictionaries-common     init               mailname         profile.d       shadow            xml
pi@poohpi:/etc $ cd /var/log
pi@poohpi:/var/log $ ls
alternatives.log       bootstrap.log    debug.3.gz      kern.log.2.gz   mail.log        mysql        user.log
alternatives.log.1     btmp             dpkg.log        kern.log.3.gz   mail.log.1      private      user.log.1
alternatives.log.2.gz  btmp.1           dpkg.log.1      lastlog         mail.log.2.gz   syslog       user.log.2.gz
apache2                daemon.log       dpkg.log.2.gz   lightdm         mail.warn       syslog.1     user.log.3.gz
apt                    daemon.log.1     exim4           mail.err        mail.warn.1     syslog.2.gz  wtmp
auth.log               daemon.log.2.gz  faillog         mail.err.1      mail.warn.2.gz  syslog.3.gz  Xorg.0.log
auth.log.1             daemon.log.3.gz  firebird        mail.err.2.gz   messages        syslog.4.gz  Xorg.0.log.old
auth.log.2.gz          debug            fontconfig.log  mail.info       messages.1      syslog.5.gz
auth.log.3.gz          debug.1          kern.log        mail.info.1     messages.2.gz   syslog.6.gz
boot.log               debug.2.gz       kern.log.1      mail.info.2.gz  messages.3.gz   syslog.7.gz
pi@poohpi:/var/log $ _
```

How to SSH into Server

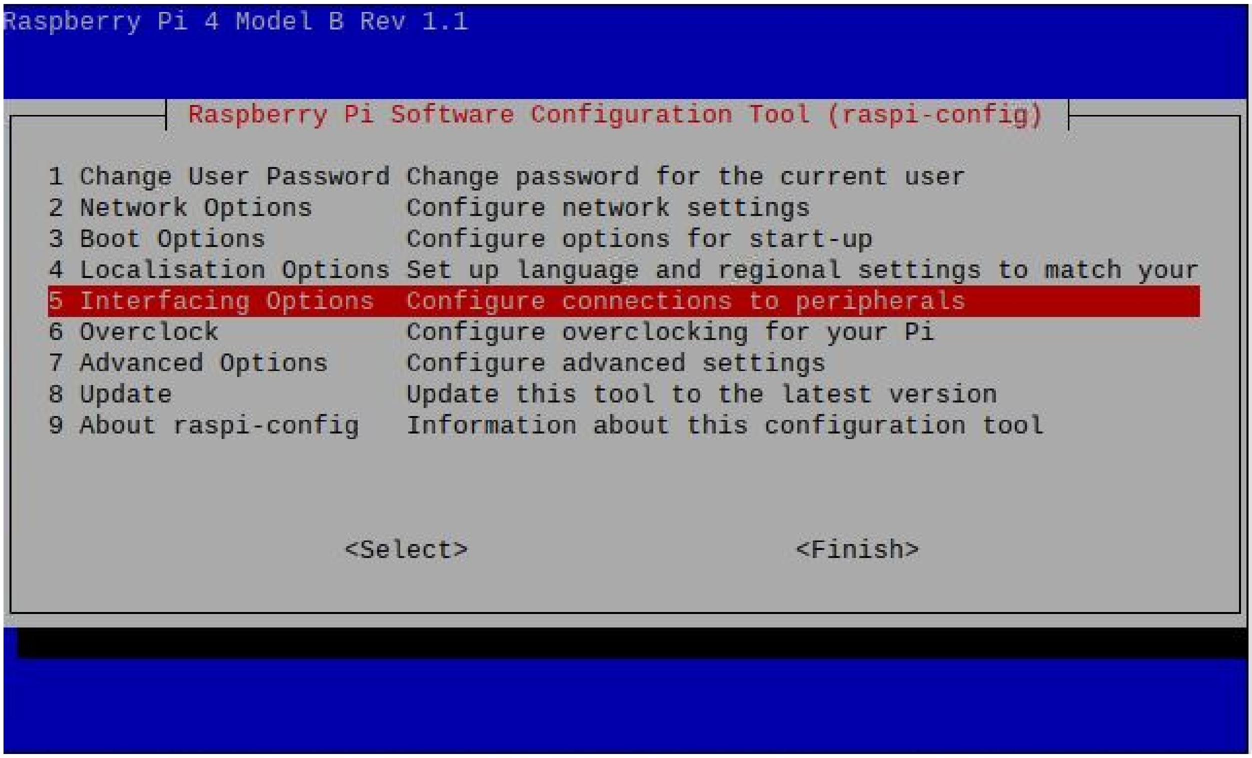
Before starting, you will need a Raspberry Pi that is connected to your LAN (WiFi). A guide to do so can be found here:
https://www.raspberrypi.org/documentation/configuration/wireless/wireless-cli.md

Once the raspberry PI is connected to the LAN, open a terminal window on the Raspberry Pi and run the following command:



```
pi@poohpi:~ $ sudo raspi-config
```

The following menu will appear. Select “Interfacing Options>SSH>Enable”:

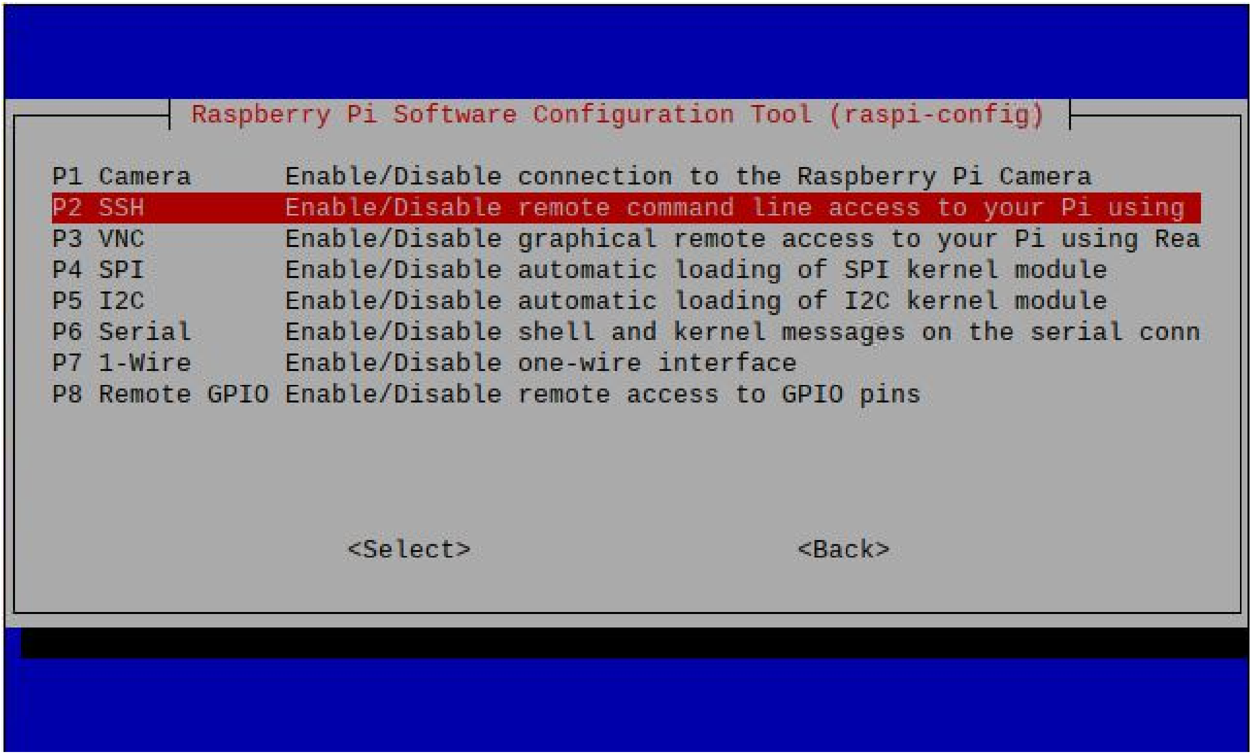


```
Raspberry Pi 4 Model B Rev 1.1

              Raspberry Pi Software Configuration Tool (raspi-config)

 1 Change User Password Change password for the current user
 2 Network Options      Configure network settings
 3 Boot Options         Configure options for start-up
 4 Localisation Options Set up language and regional settings to match your
 5 Interfacing Options  Configure connections to peripherals
 6 Overclock            Configure overclocking for your Pi
 7 Advanced Options     Configure advanced settings
 8 Update               Update this tool to the latest version
 9 About raspi-config   Information about this configuration tool

                <Select>                     <Finish>
```

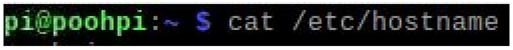


```
              Raspberry Pi Software Configuration Tool (raspi-config)

 P1 Camera      Enable/Disable connection to the Raspberry Pi Camera
 P2 SSH         Enable/Disable remote command line access to your Pi using
 P3 VNC         Enable/Disable graphical remote access to your Pi using Rea
 P4 SPI         Enable/Disable automatic loading of SPI kernel module
 P5 I2C         Enable/Disable automatic loading of I2C kernel module
 P6 Serial      Enable/Disable shell and kernel messages on the serial conn
 P7 1-Wire      Enable/Disable one-wire interface
 P8 Remote GPIO Enable/Disable remote access to GPIO pins

                <Select>                     <Back>
```

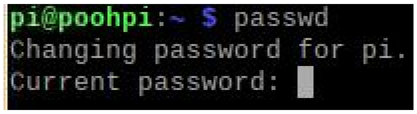
In order to connect to your Raspberry Pi from another machine, you need to know the hostname of your Raspberry Pi. This can be found by running the following command:



```
pi@poohpi:~ $ cat /etc/hostname
```

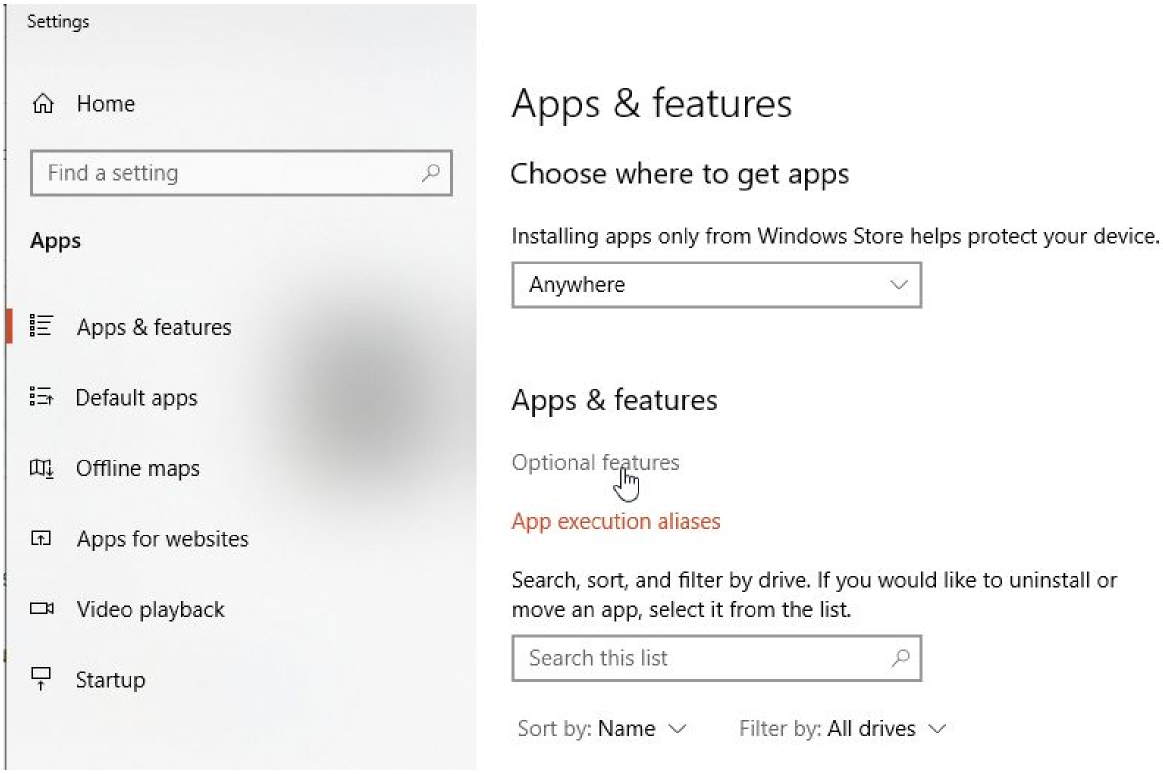
If you would like, you can change your hostname using this guide: https://thepihut.com/blogs/raspberry-pi-tutorials/19668676-renaming-your-raspberry-pi-the-hostname

We highly recommend changing your Raspberry Pi's default password (probably "raspberrypi") with the "passwd" command. You will be prompted for your current password and a new password:



```
pi@poohpi:~ $ passwd
Changing password for pi.
Current password: 
```

Once all of this is taken care of we can SSH into the Raspberry Pi now. (This is assuming you are a Windows 10 user) Search for "Apps and Features" on your Windows machine. Once you are in the "Apps and Features" menu, click "Optional Features", and install "Open SSH Server."

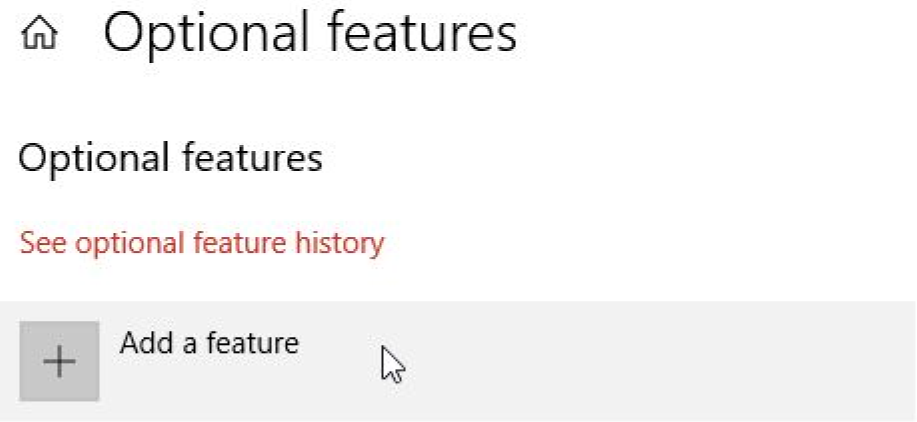


Installing apps only from Windows Store helps protect your device.

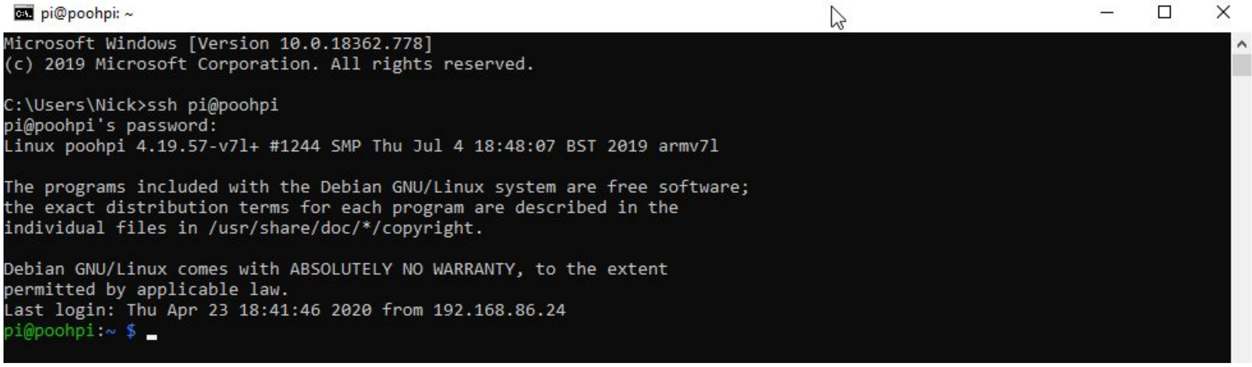
Anywhere

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

If you do not see “Open SSH Server” in your menu, click “Add Feature” and look for it there:



Once this is installed, restart your computer, and open a Command Prompt. Type the following command: “ssh [user]@[hostname]”
[user] will most likely be “pi” and we know your hostname from the initial setup of the Raspberry Pi from above.



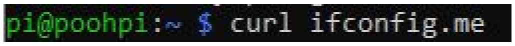
```
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Nick>ssh pi@poohpi
pi@poohpi's password:
Linux poohpi 4.19.57-v7l+ #1244 SMP Thu Jul 4 18:48:07 BST 2019 armv7l

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.
Last login: Thu Apr 23 18:41:46 2020 from 192.168.86.24
pi@poohpi:~ $ 
```

Congratulations, you have connected the server via SSH. To connect to the server from outside the LAN, you will need to know your public IP address. To find this, you can run the following command from the SSH terminal: .

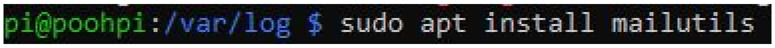


```
pi@poohpi:~ $ curl ifconfig.me
```

When you run the SSH command from outside your LAN, you can replace your hostname with the IP returned by this command.

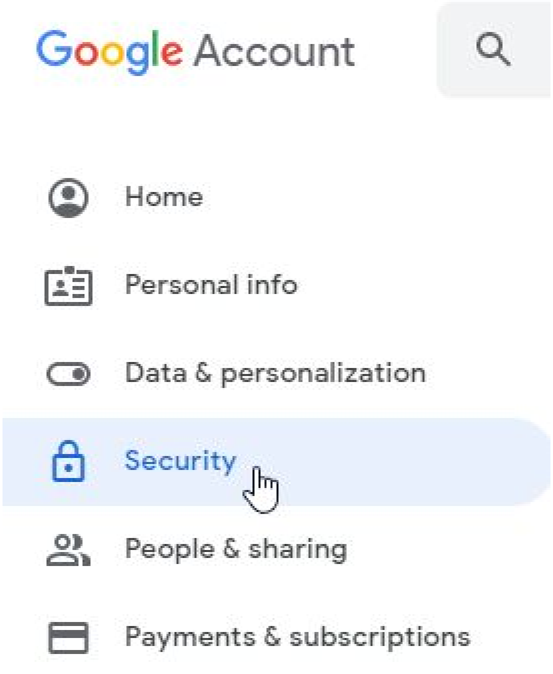
Setting up mailutils for email alerts

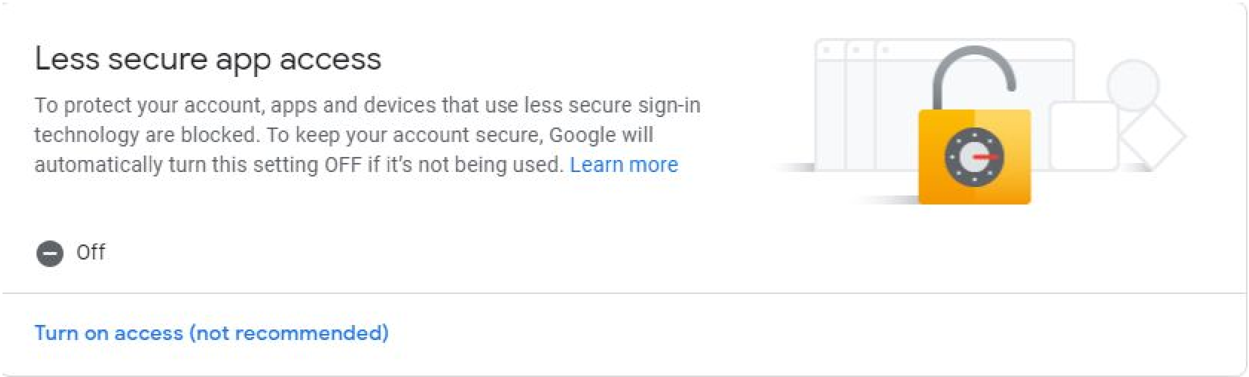
Run following command on server:



```
pi@poohpi:/var/log $ sudo apt install mailutils
```

Create a gmail account (do not recommend using your own) and enable less secure apps:



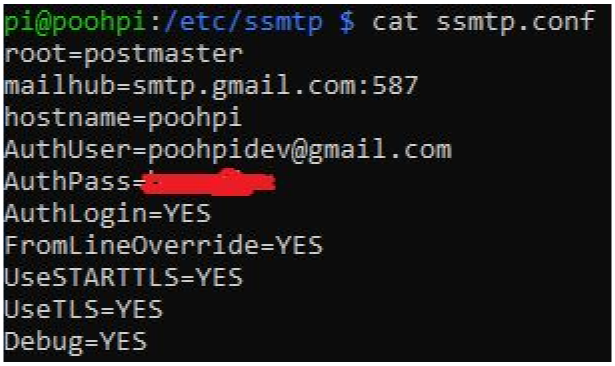


Less secure app access

To protect your account, apps and devices that use less secure sign-in technology are blocked. To keep your account secure, Google will automatically turn this setting OFF if it's not being used. Learn more

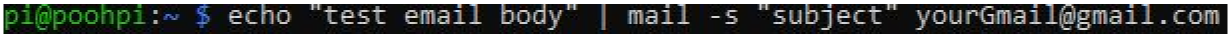
Off

Edit ‘ssmtp.conf’ to resemble the following:



```
pi@poohpi:/etc/ssmtp $ cat ssmtp.conf
root=postmaster
mailhub=smtp.gmail.com:587
hostname=poohpi
AuthUser=poohpidev@gmail.com
AuthPass=[redacted]
AuthLogin=YES
FromLineOverride=YES
UseSTARTTLS=YES
UseTLS=YES
Debug=YES
```

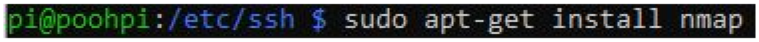
Then run the following command to test an email:



```
pi@poohpi:~ $ echo "test email body" | mail -s "subject" yourGmail@gmail.com
```

Installing Nmap

Nmap is a useful tool that will allow us to scan Networks of people trying to access the server, but first we need to install it by running this command:



```
pi@poohpi:/etc/ssh $ sudo apt-get install nmap
```

Once nmap is installed, you can read how to use it for different scenarios here:
https://hackertarget.com/nmap-tutorial/