Lab Assignment

Cybersecurity Professional Program

Linux Security

Services and Hardening

LNX-05-L3

Securing Services

Lab Objective

Understand how to harden and secure SSH and FTP and how to back up the Samba configuration file.

Lab Mission

Make existing installed services more secure and less vulnerable and learn about Windows tools.

Lab Duration

40–50 minutes

Requirements

- General knowledge of commands
- Knowledge of system-related commands

Resources

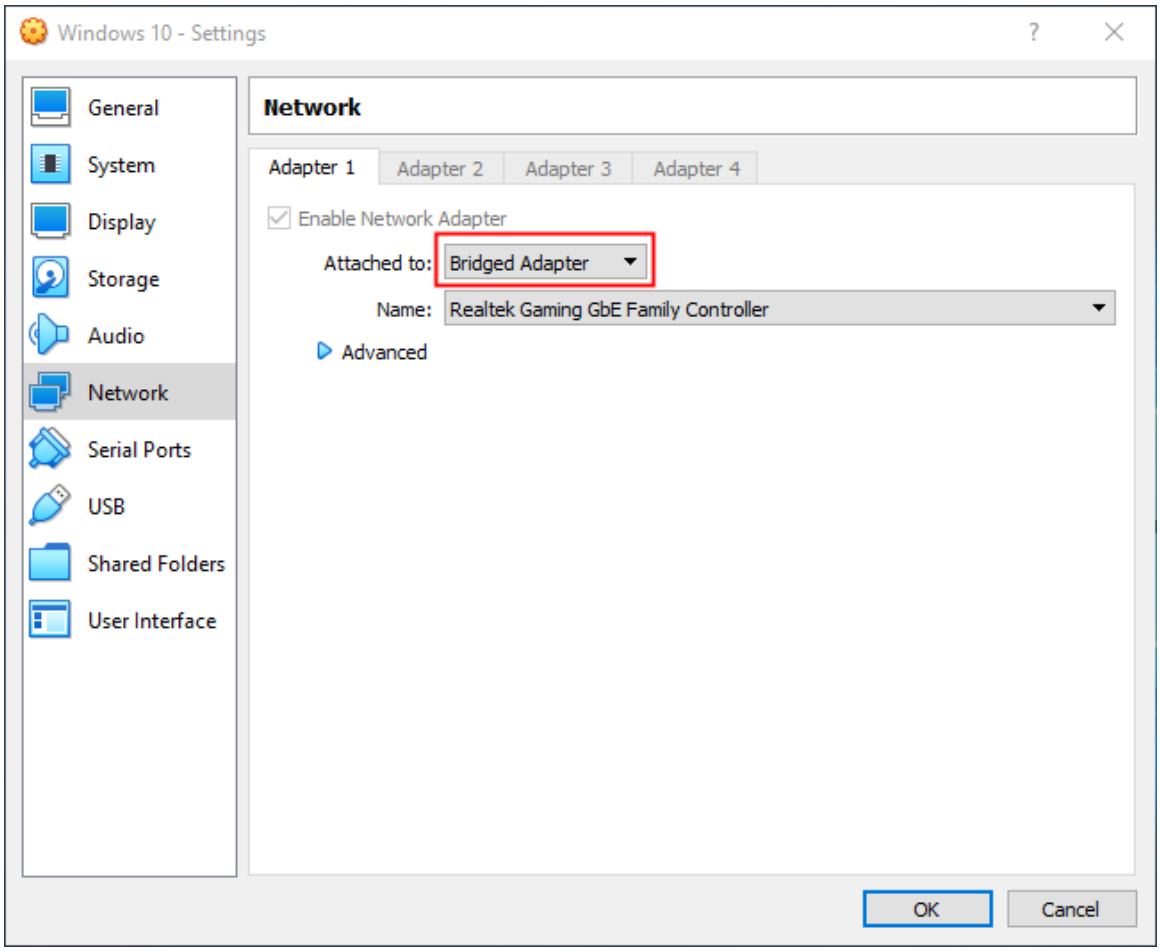
- Environment & Tools
  - VirtualBox
    - Debian
  - Windows
- Extra Lab Files
  - ***putty.zip***
  - ***WinSCP-5.19.5-Setup***

Lab Task 1: SSH Hardening

Enhance and secure SSH by setting connection limitations and port configuration. Before starting, make sure the Windows host and Debian VMs are turned on and have connectivity with each other and the internet.

1. Follow the **Installing Guest Additions** section in the Windows 10 installation guide to install guest additions in your Windows VM.
2. Make sure the NIC in both the Debian and Windows machines is set to ***Bridged Adapter***.

   Note: If you are unable to receive an IP from DHCP, please switch from ***Bridged Adapter*** to ***NAT Network***.



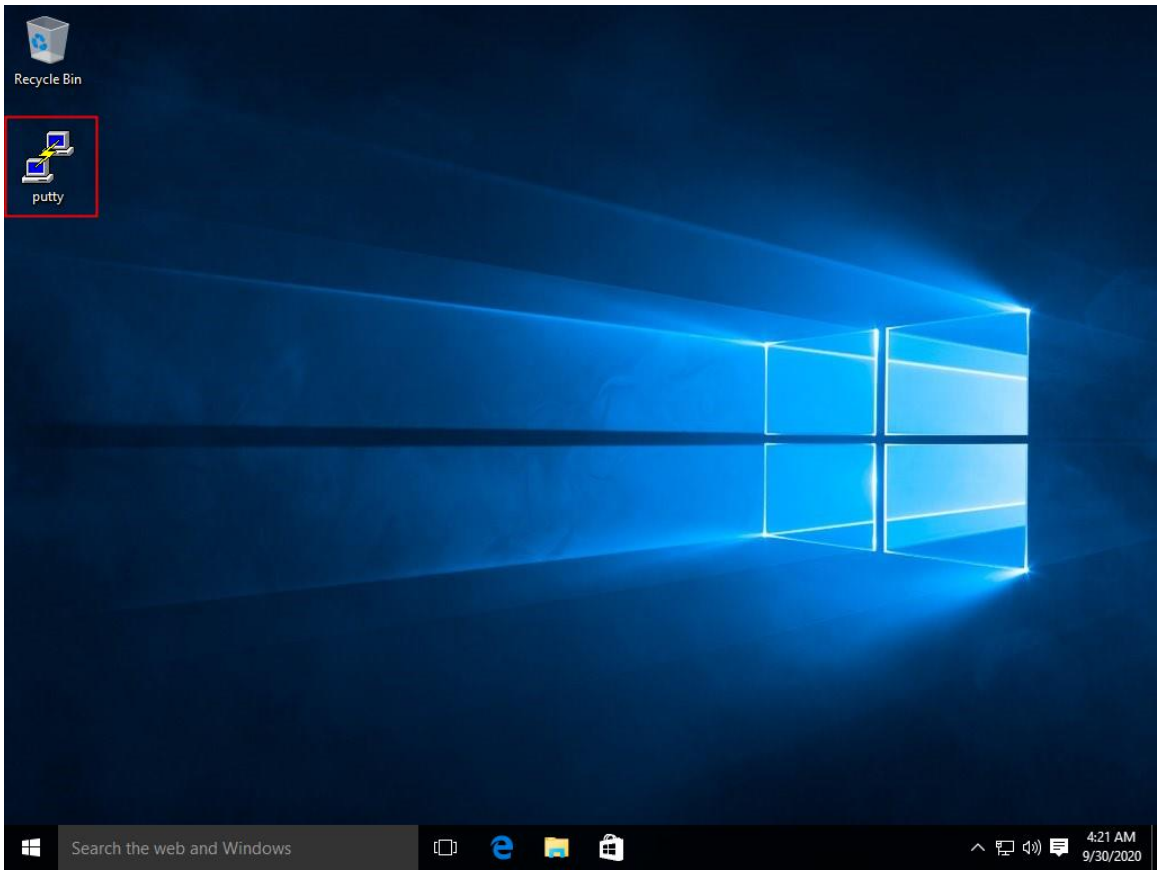
3 Open the terminal in Debian and use the ***su –*** command to switch to the root user.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
john@debian:~$ su -
Password:
root@debian:~#
```

4 Use the ***service ssh start*** command to start SSH service. Verify it is active using the ***service ssh status*** command.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
root@debian:~# service ssh start
root@debian:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; ena
   Active: active (running) since Wed 2020-09-30 06:05:
```

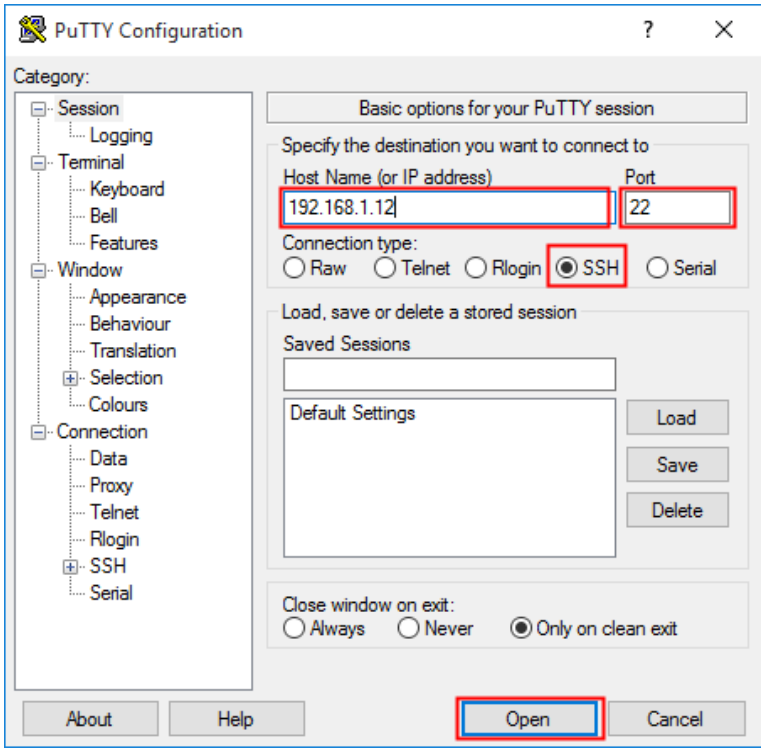
5 Copy the provided ***putty.exe*** file to the Windows machine.



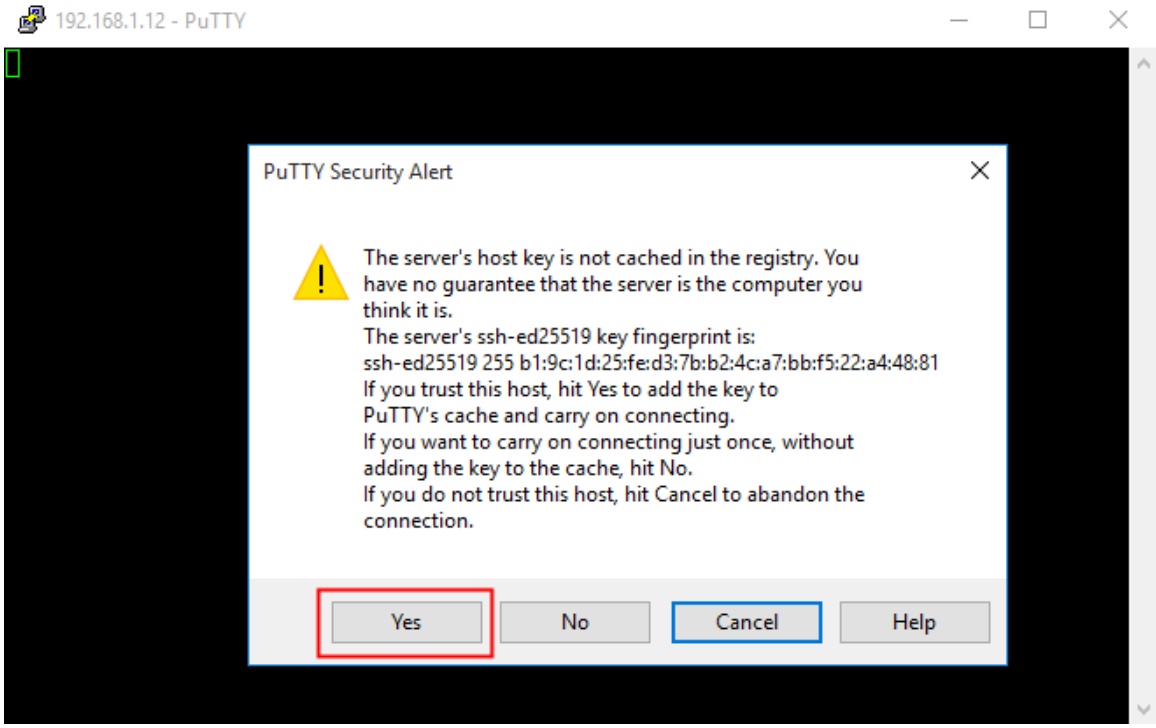
6 Check the IP address in your Debian machine using the ***ip a*** command.

```
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gro
up default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP group default qlen 1000
    link/ether 08:00:27:6d:00:ff brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic noprefi
xroute enp0s3
       valid_lft 3593sec preferred_lft 3593sec
    inet6 2a00:a040:19c:a2e7:e8fe:ede2:be0:a25f/64 scope global tempora
ry dynamic
       valid_lft 599987sec preferred_lft 81441sec
    inet6 2a00:a040:19c:a2e7:a00:27ff:fe6d:ff/64 scope global dynamic m
ngtmpaddr noprefixroute
       valid_lft 808164sec preferred_lft 330574sec
    inet6 fe80::a00:27ff:fe6d:ff/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@debian:~#
```

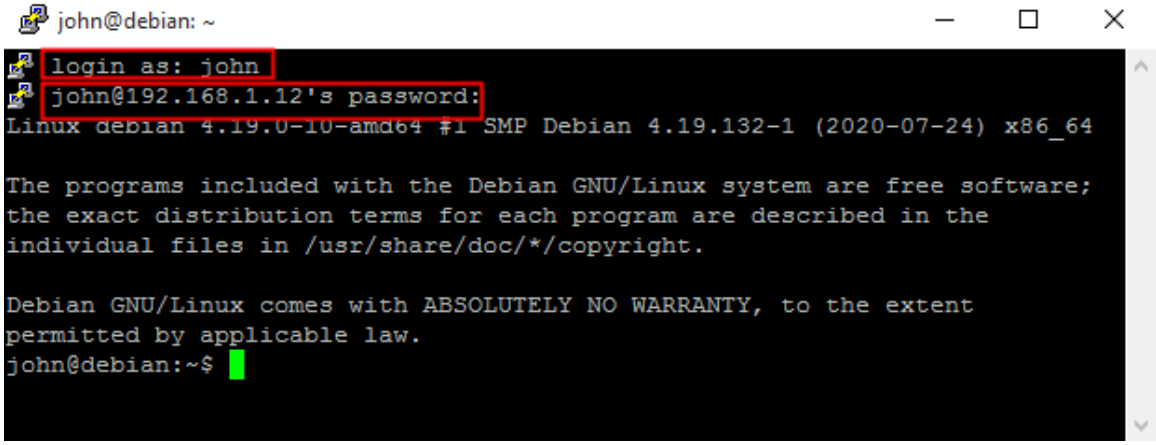
7 In the Windows machine, double-click ***putty*** to start it. Insert Debian's IP address on port 22 and click **Open** to open a connection via SSH.



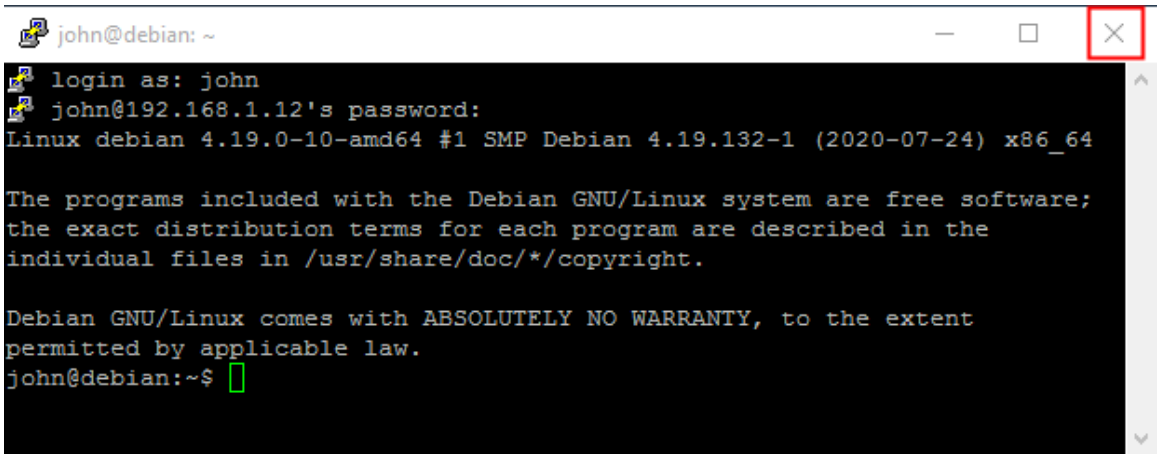
8 Click **Yes** in the **Security Alert** window.



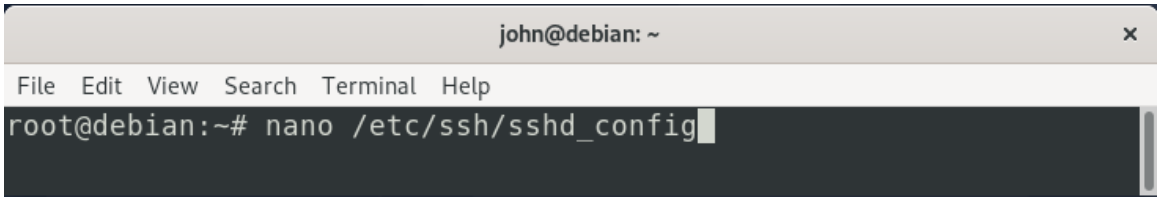
9 Provide the name and password of your Debian user and verify the connection is established.



10 Close the SSH connection.



11 In the Debian machine, use the command **sudo *nano /etc/ssh/sshd_config*** to open the service's configuration file.



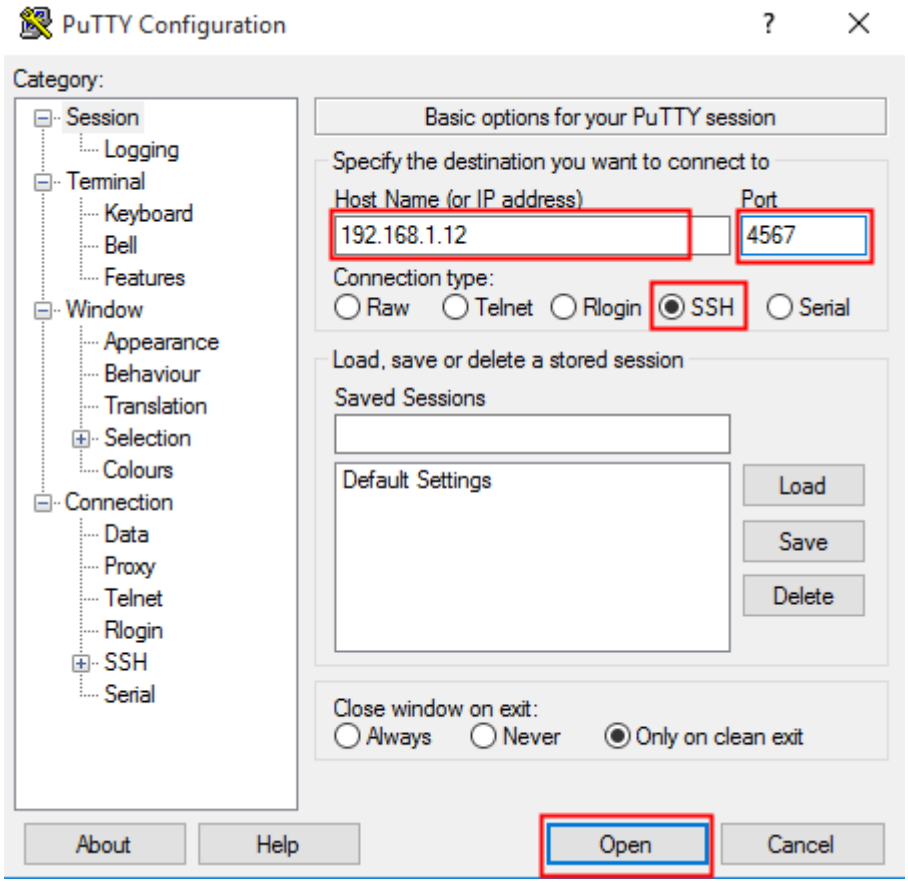
12 Use ***ctrl + w*** to search for the word *port*. Uncomment it and change the number to **4567**. This will change the connection port to the service. Save and exit the file.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 3.2          /etc/ssh/sshd_config          Modified

# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options overr$
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 4567
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell
```

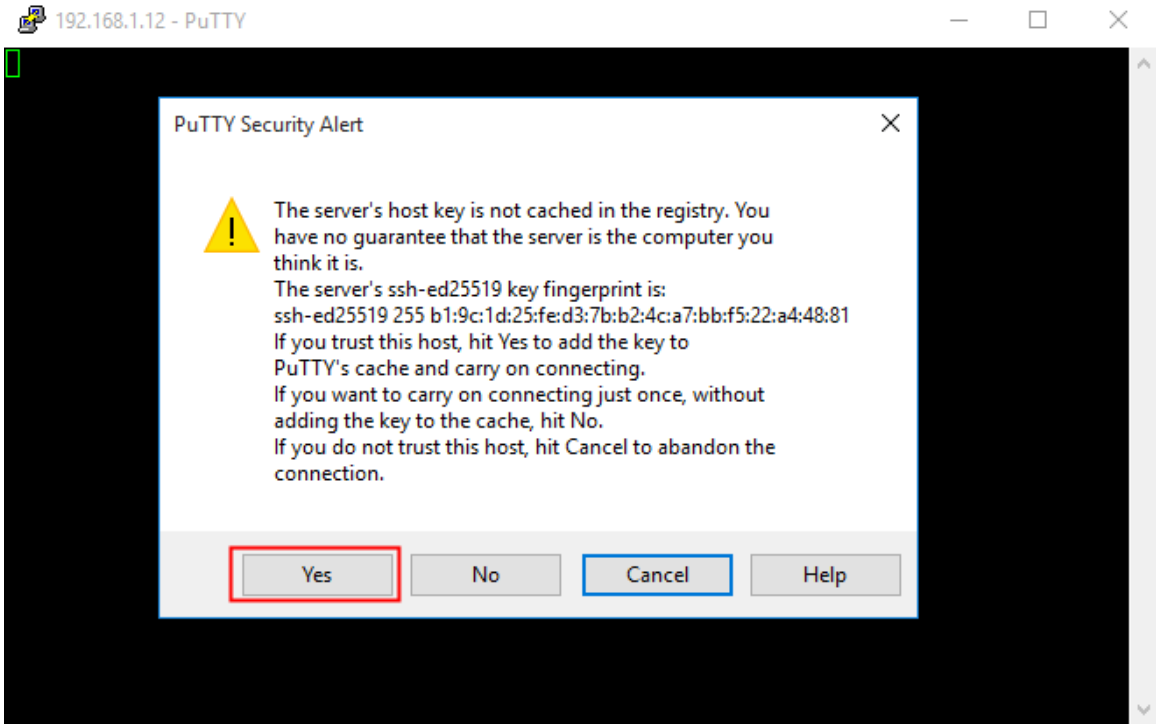
13 Use the command ***service ssh restart*** and then ***service ssh status*** to verify the service is active on port **4567**.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
root@debian:~# service ssh restart
root@debian:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-01-12 09:22:52 EST; 5s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 6389 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 6390 (sshd)
    Tasks: 1 (limit: 1138)
   Memory: 1.1M
   CGroup: /system.slice/ssh.service
           └─6390 /usr/sbin/sshd -D

Jan 12 09:22:52 debian systemd[1]: Starting OpenBSD Secure Shell server...
Jan 12 09:22:52 debian sshd[6390]: Server listening on 0.0.0.0 port 4567.
Jan 12 09:22:52 debian sshd[6390]: Server listening on :: port 4567.
Jan 12 09:22:52 debian systemd[1]: Started OpenBSD Secure Shell server.
```

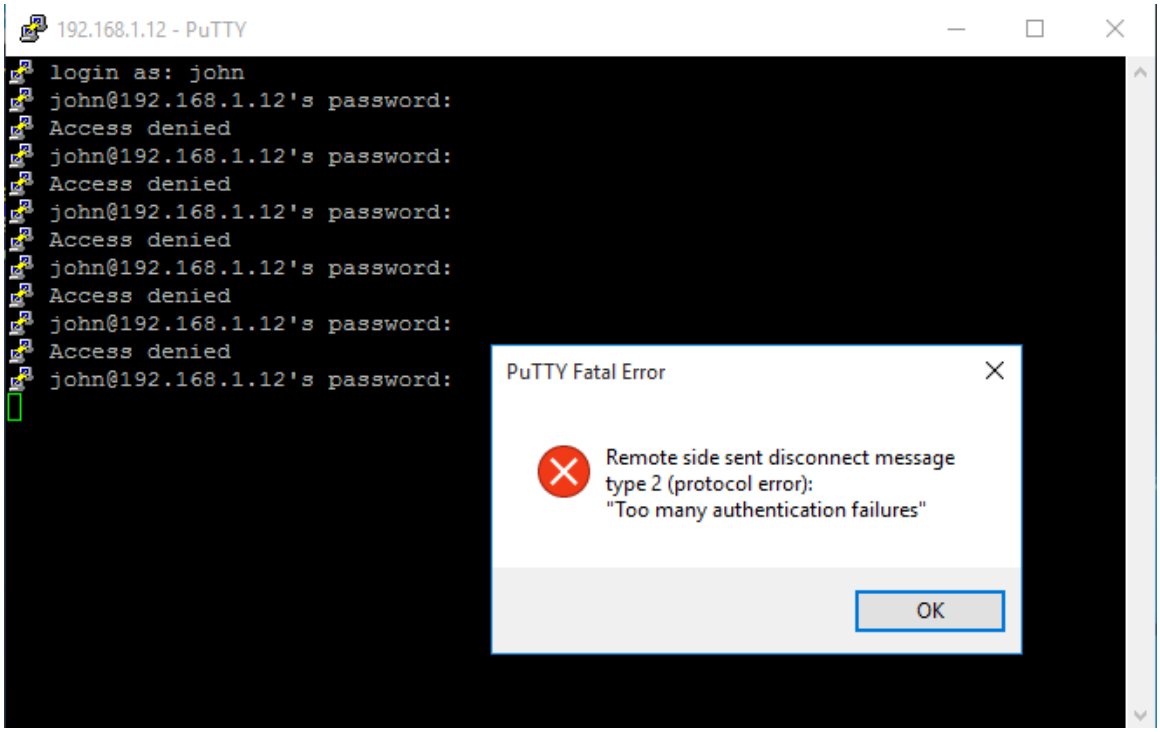
14 Open **putty** again and connect this time to port 4567.



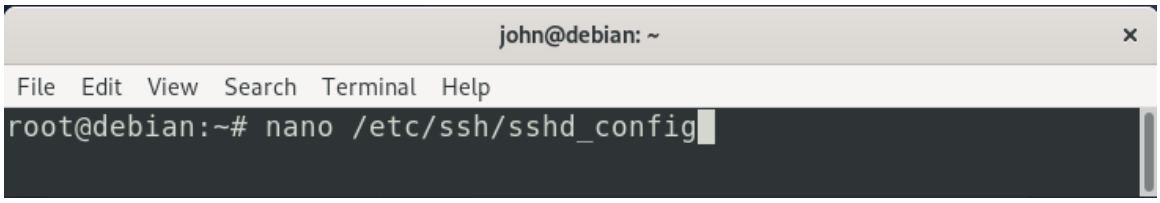
15 Click **Yes** in the alert window.



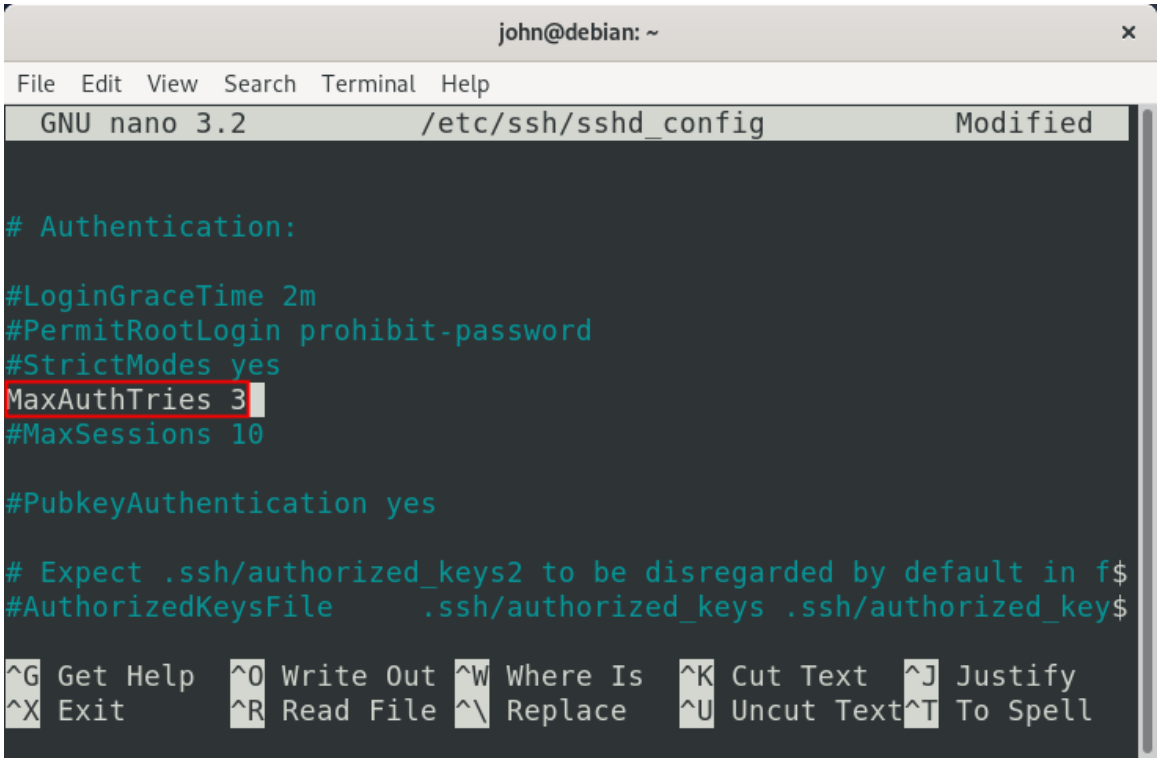
16 Provide your username but then insert an incorrect password six times and note the error message.



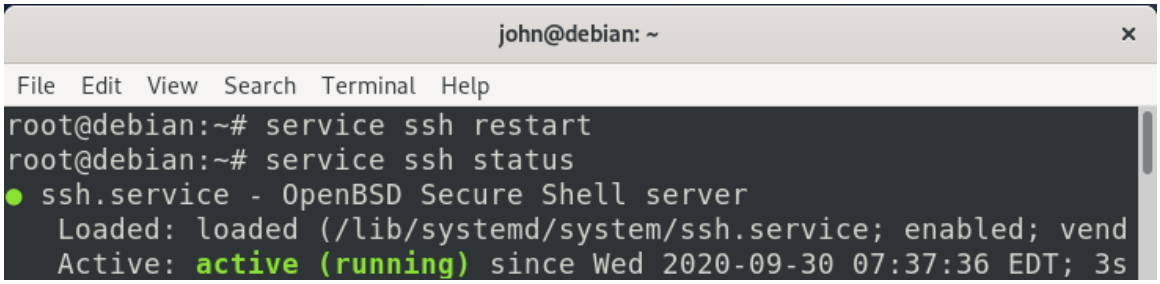
17 In the Debian machine, use the command ***nano /etc/ssh/sshd_config*** to open the service's configuration file.



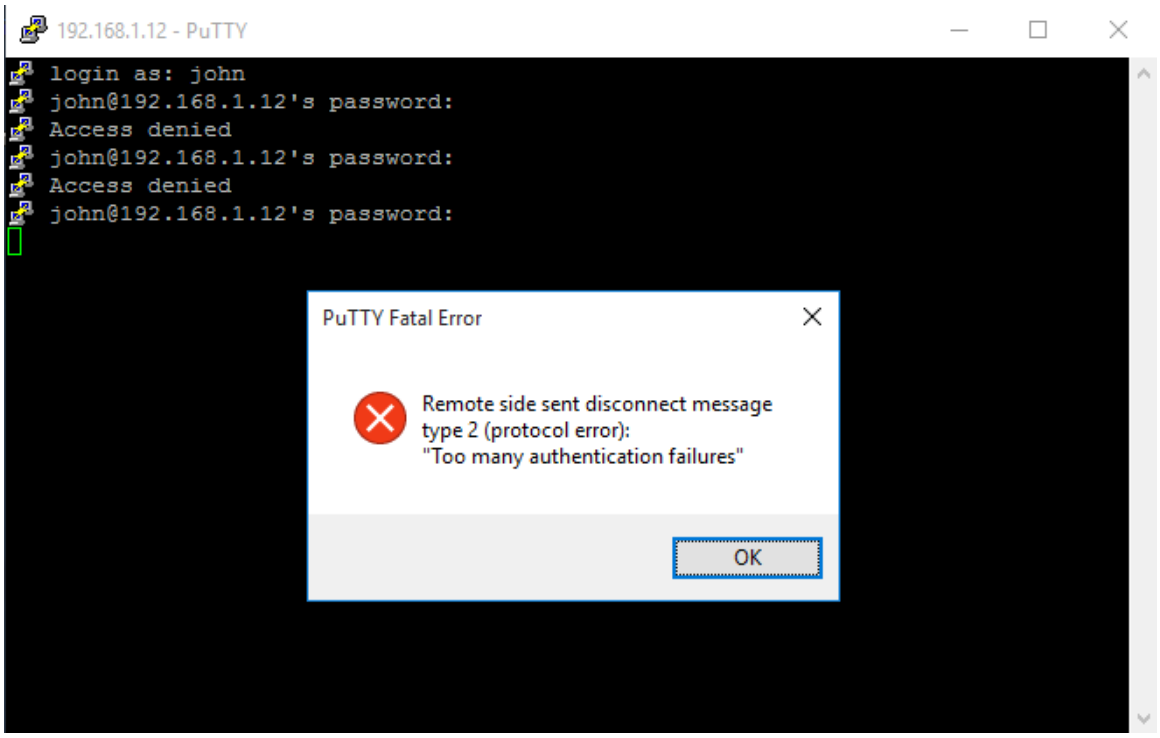
18 Use ***ctrl + w*** to search for the word *MaxAuthTries*. Uncomment it and change the number to **3**. This will change the number of permitted login attempts. Save and exit the file.



19 Use the command ***service ssh restart*** and then ***service ssh status*** to verify the service is active.



20 Connect again to the SSH service via **putty** and verify the login failure count was updated.



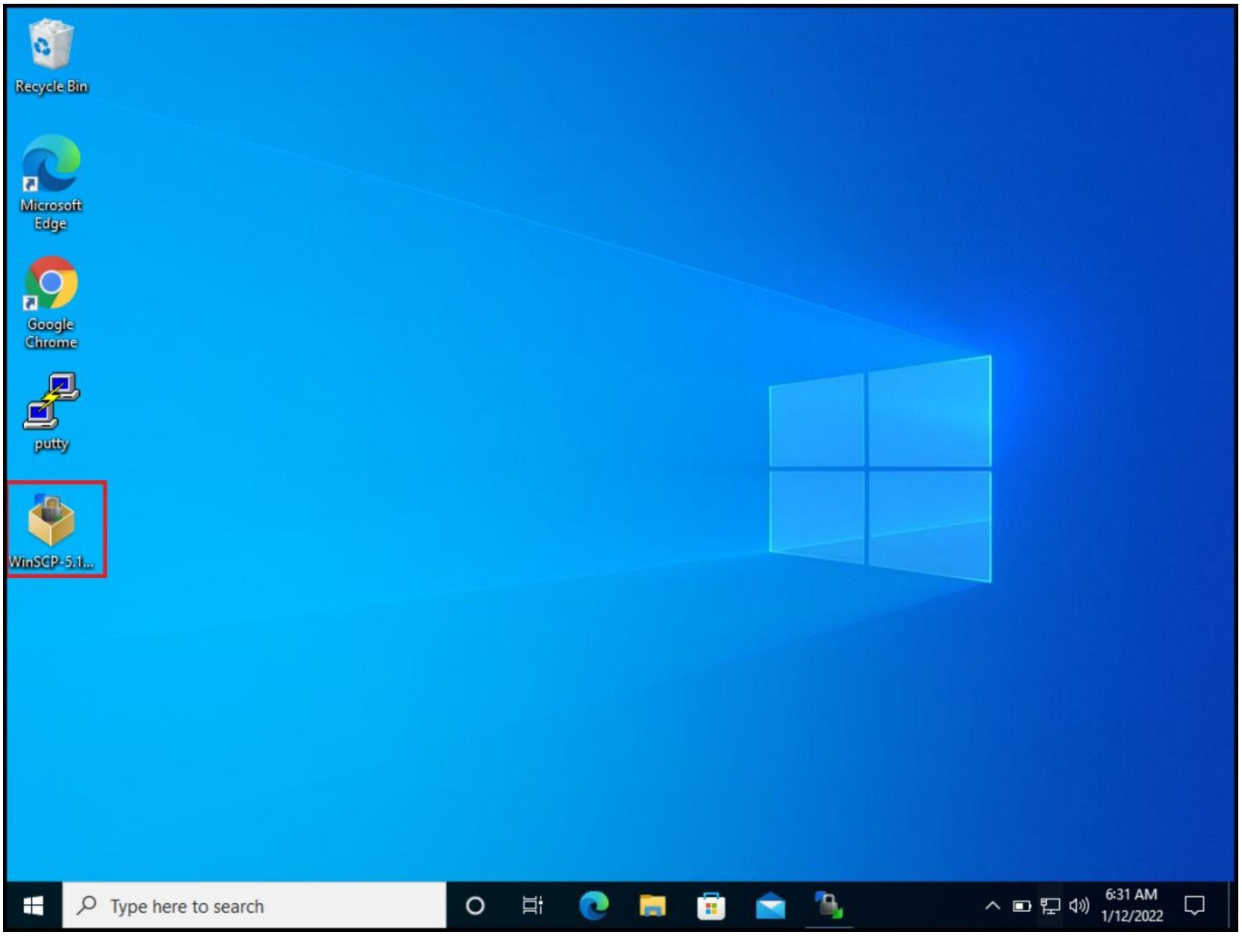
21 Type **nano /etc/ssh/sshd_config** and change the port number to **22** with a hashtag to have the default value. **Important**: Read the blue text.

```
File  Edit  View  Search  Terminal  Help
  GNU nano 3.2                    /etc/ssh/sshd_config                    Modified

#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.


#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

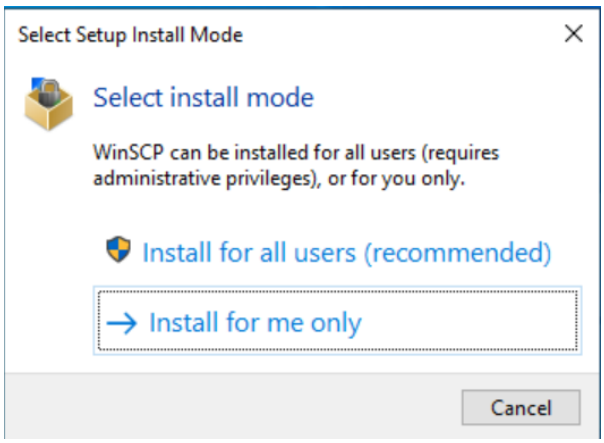
Lab Task 2: WinSCP Obfuscation

Change the port number for the FTP connection and connect using WinSCP.

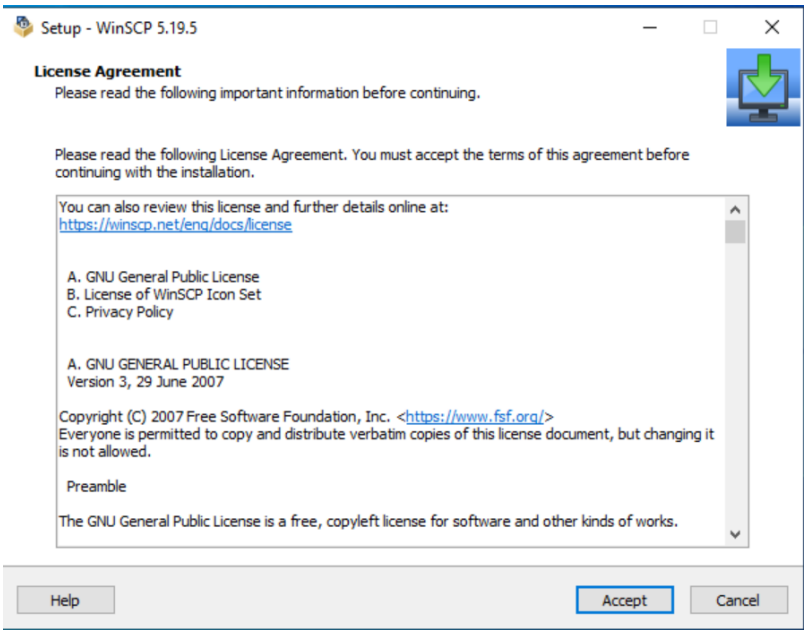
1 Copy the WinSCP installation file to your Windows machine and double-click it.



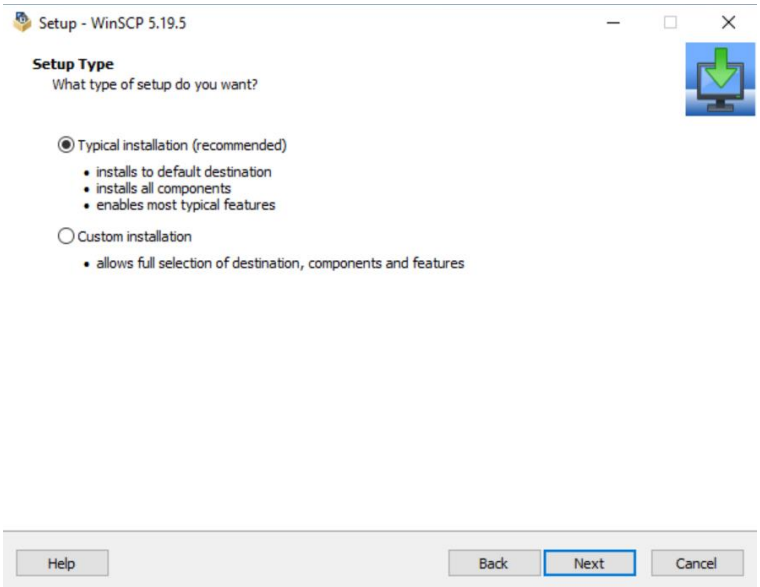
2 Click **Install for me only.**



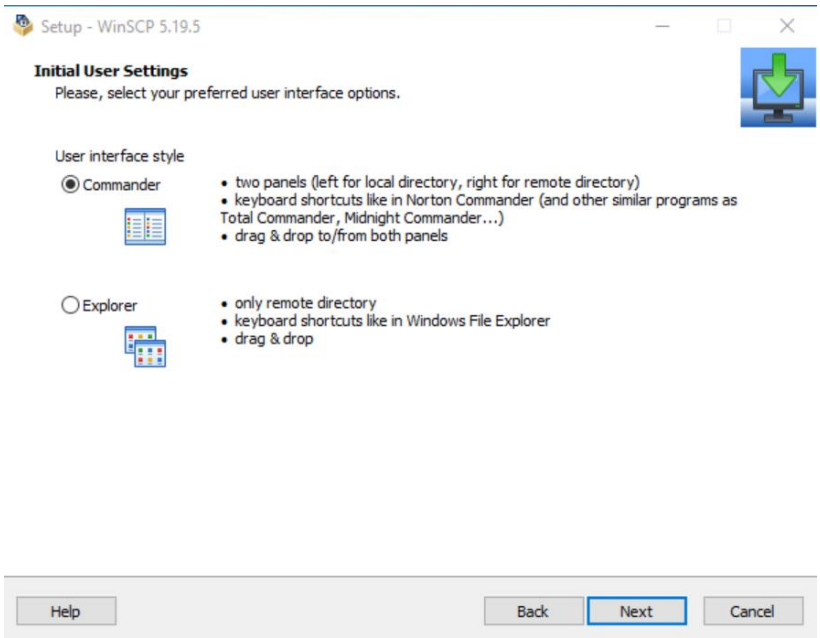
3 Click **Accept** for the license agreement.



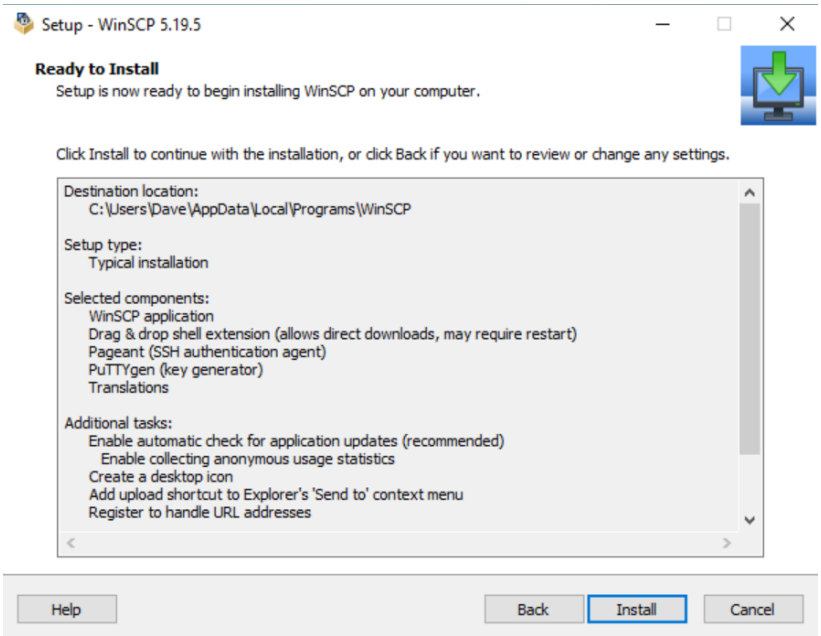
4 For the setup type, choose ***Typical installation*** and click **Next**.



5 In the initial user settings, select ***Commander*** and click **Next**.

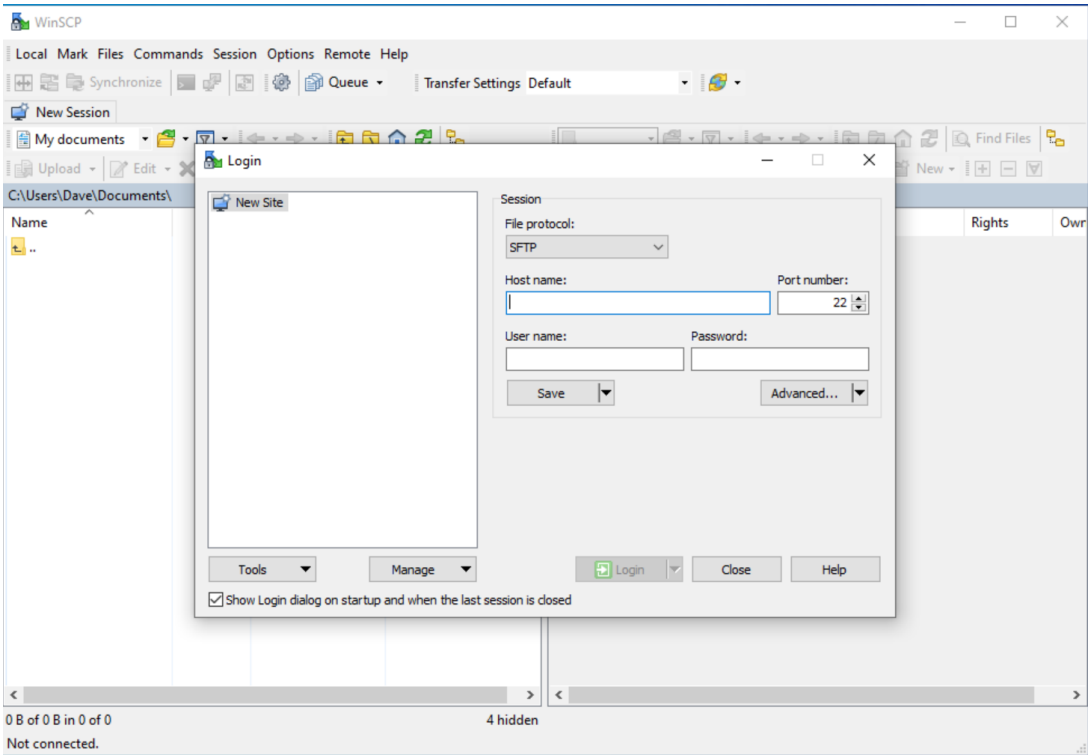


6 After **Ready to Install**, click **Install**.

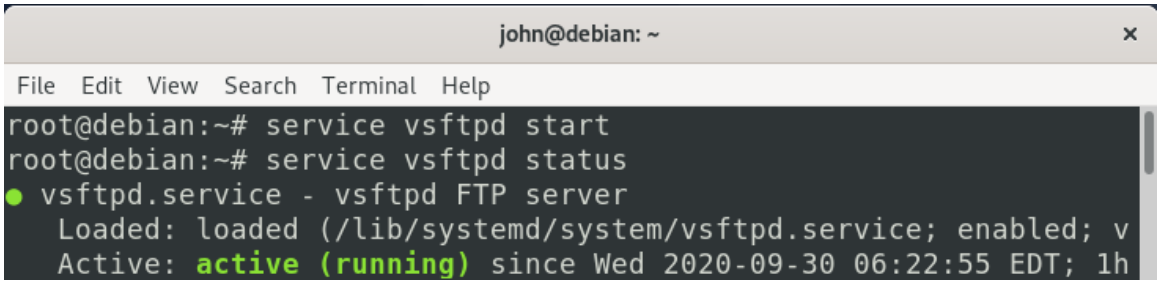


7 Uncheck the ***Open Getting started page*** and click **Finish**.

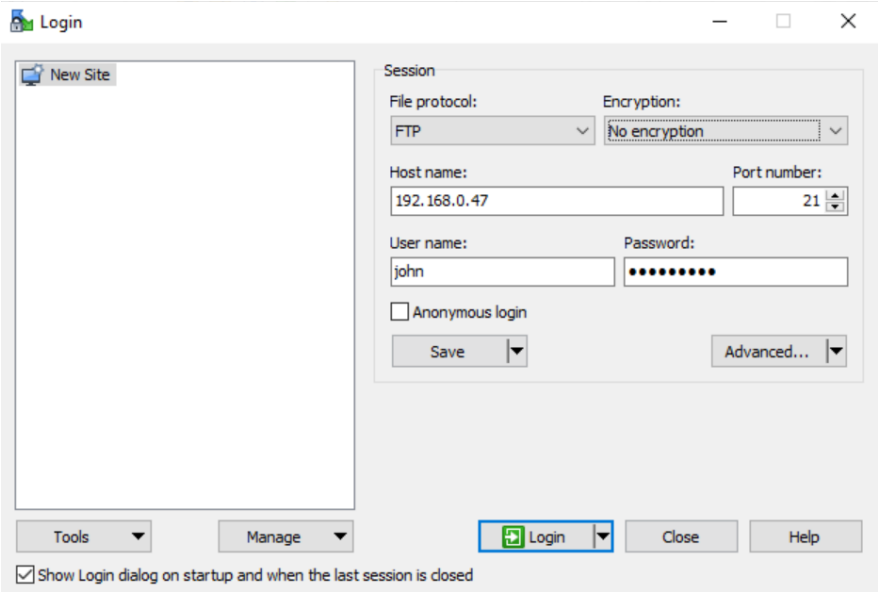
8 WinSCP will open.



9 Use the command ***service vsftpd start*** to start the FTP server and then use ***service vsftpd status*** to verify the service is active.



10 In the WinSCP host name, enter the IP address of the Debian machine and then enter your username and password. The port will be 21 for FTP. Click **Login**.



11 In the Debian VM, use the command ***nano /etc/vsftpd.conf*** to open the service's configuration file.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
root@debian:~# nano /etc/vsftpd.conf
```

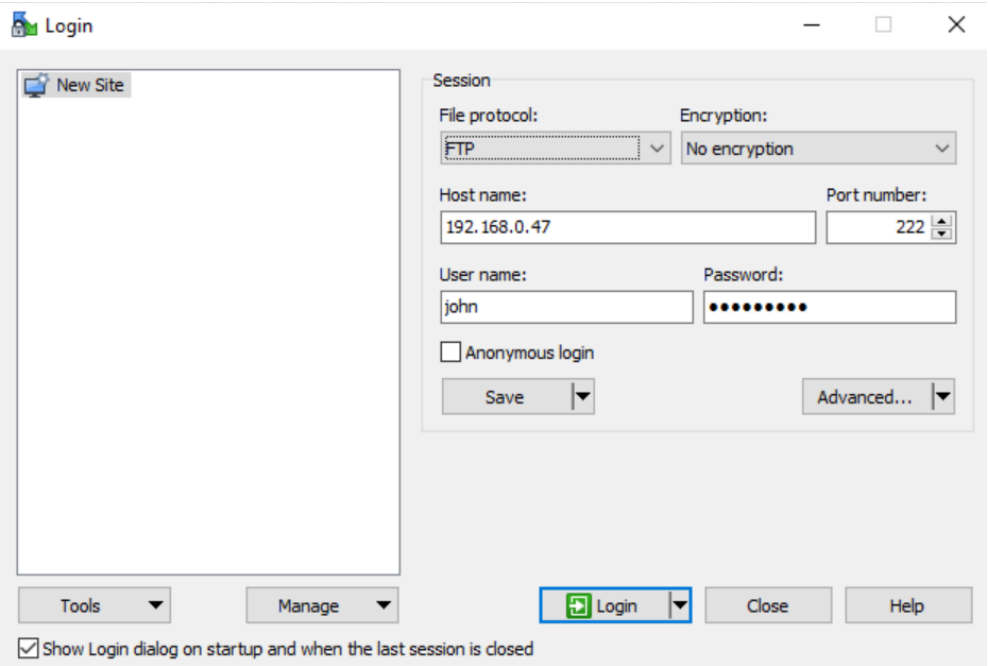
12 Use ***ctrl + w*** to search for *listen=NO* and add a line under ***listen_port=222***. Save and exit the file.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 3.2                    /etc/vsftpd.conf

# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
listen_port=222
```

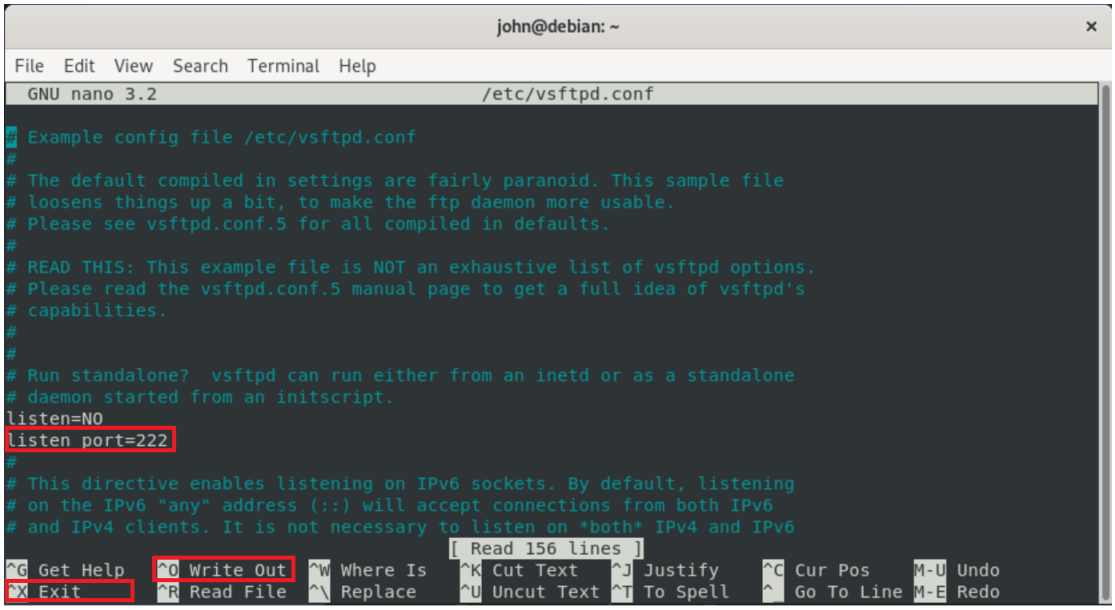
13 Use the command ***service vsftpd restart*** to restart the vsftpd service and verify it is running using the ***service vsftpd status*** command. If it fails, stop the service and start it again.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
root@debian:~# service vsftpd restart
root@debian:~# service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; v
   Active: active (running) since Wed 2020-09-30 08:44:02 EDT; 3s
```

14 Establish a new connection via WinSCP on port 222.



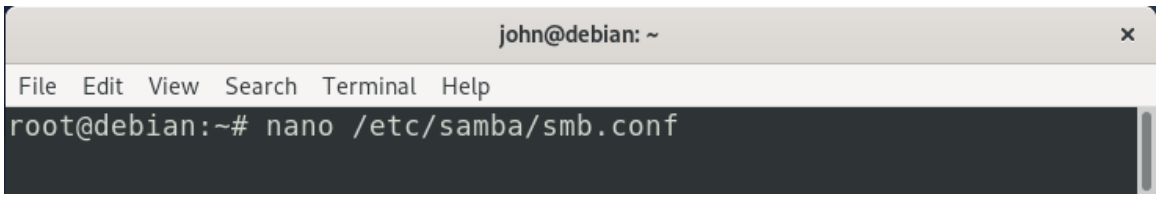
15 Remove ***Listen_port=222*** to set vsftpd back to the default.
Important: Read the blue text.



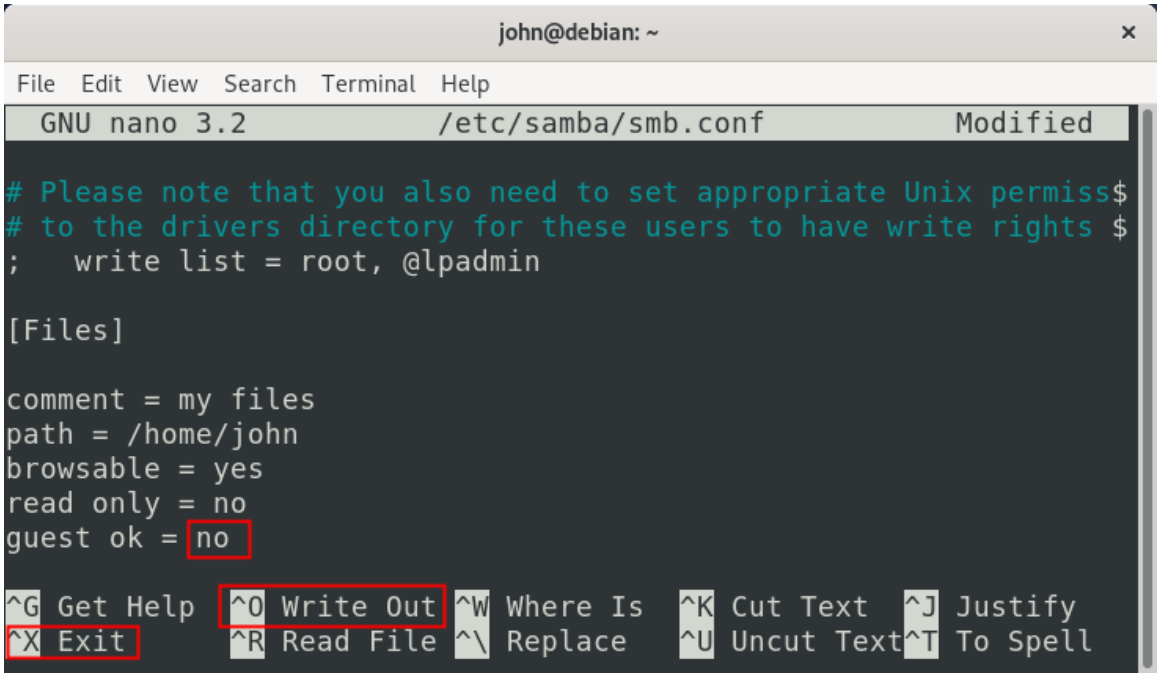
Lab Task 3: Samba Hardening

Back up the Samba configuration file.

1. In the Debian VM, use the command ***nano /etc/ samba/smb.conf*** to open the service's configuration file.



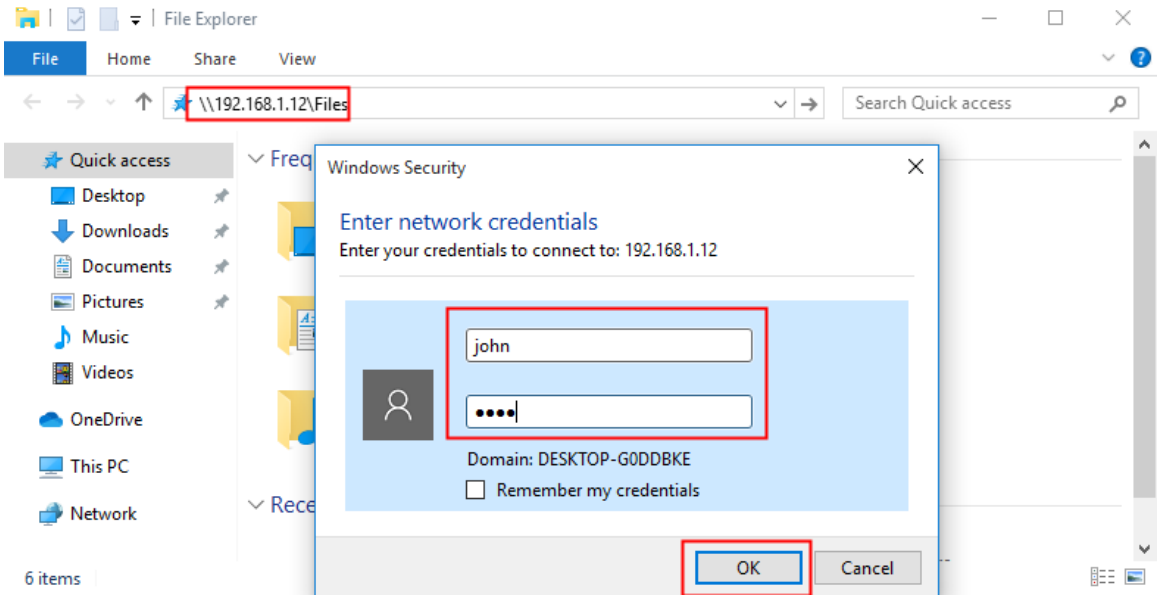
2. At the bottom of the file, change the **guest ok** option to **no**. This will prevent anyone from connecting to the share without providing credentials.
Save and exit the file.



3 Use the command ***service smbd start*** and then ***service smbd status*** to verify the service is active.

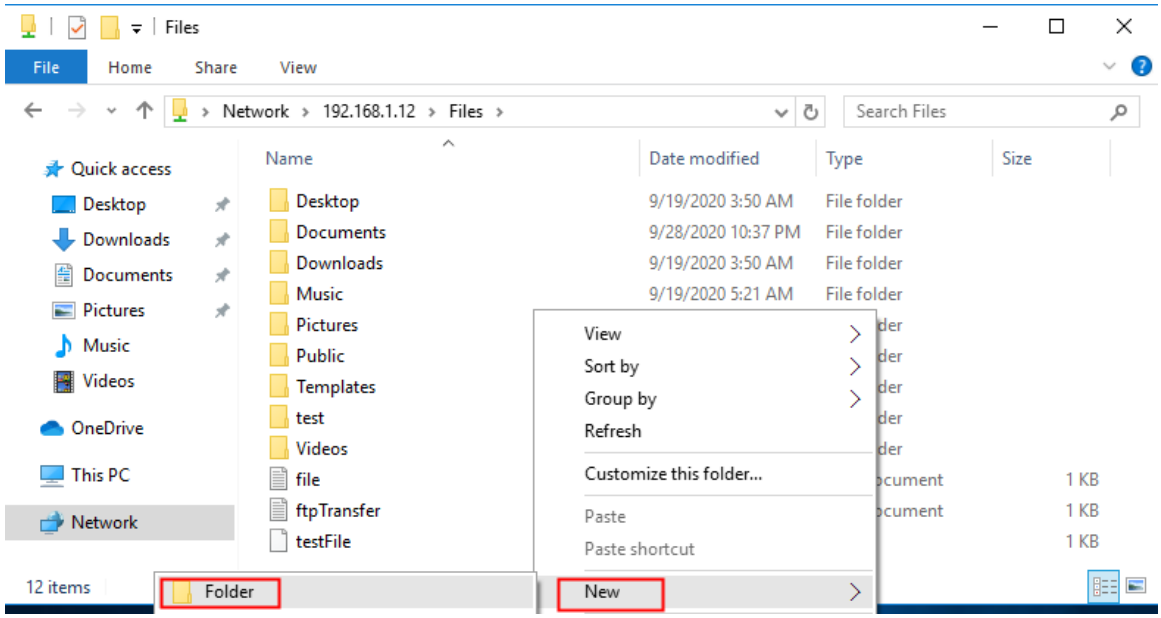
```
john@debian: ~
File  Edit  View  Search  Terminal  Help
root@debian:~# service smbd start
root@debian:~# service smbd status
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-01-12 10:06:52 EST; 54min ago
```

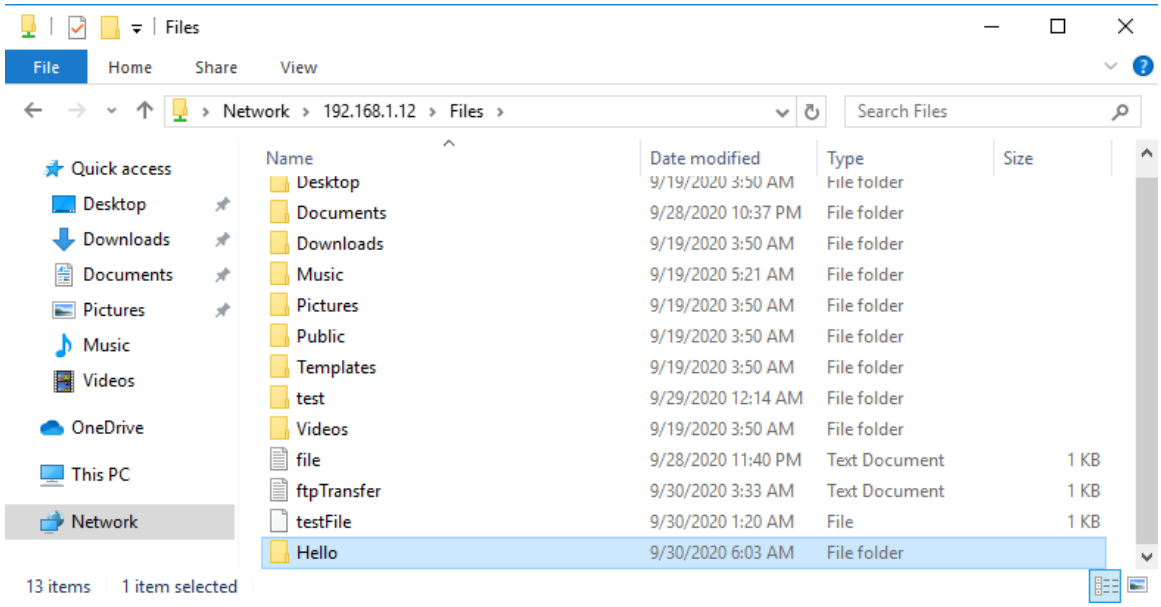
4 Open File Explorer in your Windows machine and try to access the **Files** share again via ***\\[Debian IP]\Files***. In the window that appears requesting credentials, enter the required data and click **OK**.



5 Right-click in the share and create a new folder named ***Hello***.

Note: You can write inside the share.





6 In the Debian machine, open smb's configuration file again using the ***nano /etc/samba/smb.conf*** command. Go to the bottom of the page and change **read only** to **yes**. Save and exit the file.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 3.2            /etc/samba/smb.conf            Modified

# to the drivers directory for these users to have write rights $
;   write list = root, @lpadmin

[Files]

comment = my files
path = /home/john
browsable = yes
read only = yes
guest ok = no

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell
```

7 Use the command ***service smbd restart*** and then ***service smbd status*** to verify the service is active.

```
john@debian: ~
File  Edit  View  Search  Terminal  Help
root@debian:~# service smbd restart
root@debian:~# service smbd status
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; ven
   Active: active (running) since Wed 2020-09-30 08:57:22 EDT; 37
```

8 Try again to create a folder in the share from File Explorer. Note the alert indicating you need permission to perform this action.