Services and Firewalls

CMPUT 333 – Assignment 2, Parts 1 & 2

HTTP, FTP and TFTP Services

HTTP Service

- Must be on the Windows VM
- Recommended software: Apache
  - Download httpd-2.2.25-win32-x86-openssl-0.9.8y.msi from https://archive.apache.org/dist/httpd/binaries/win32/
  - This is a version with openssl that will be usefull for the sliding part

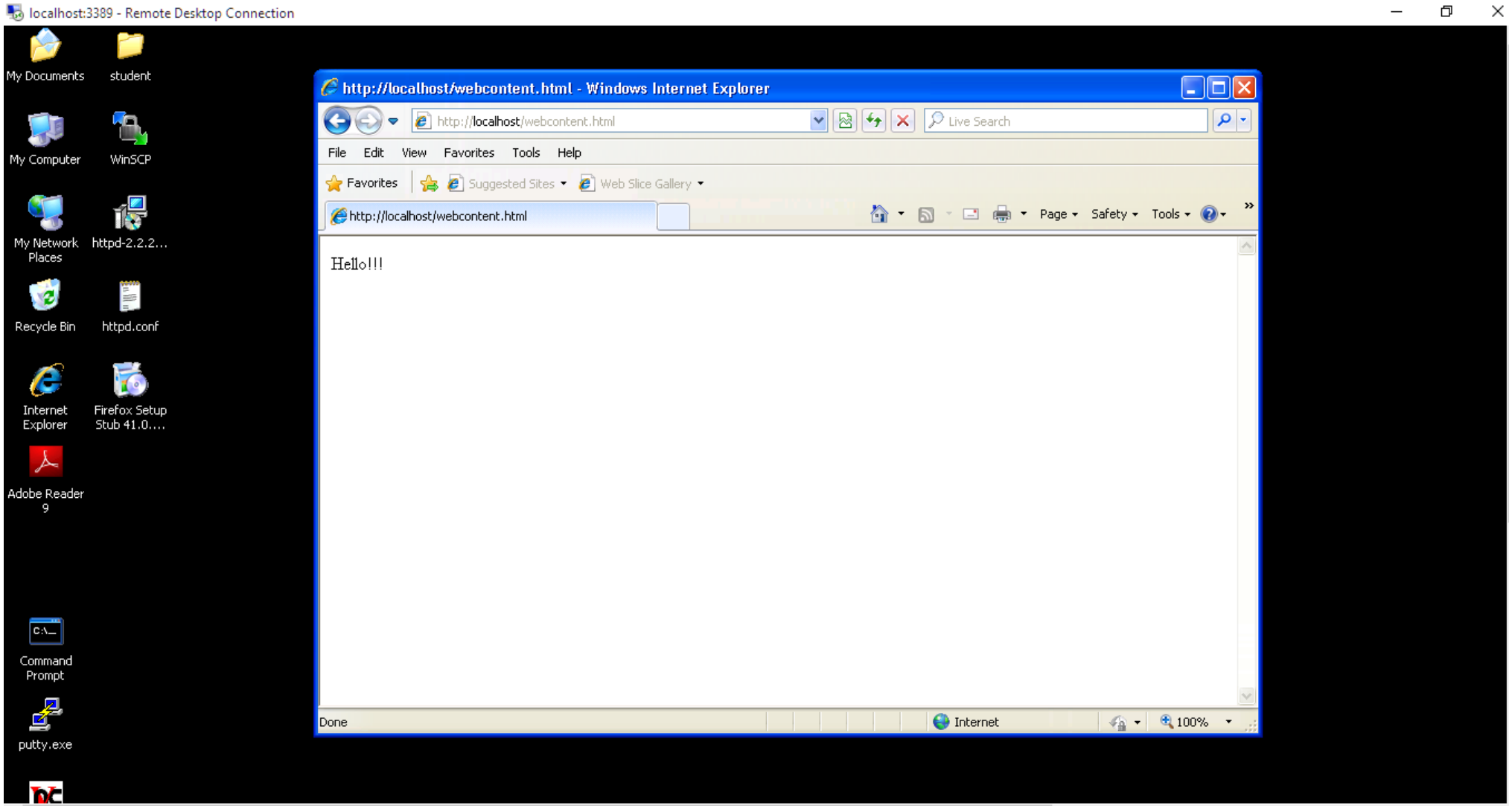
- The Windows users should use the windows authentication credentials and system to gain access to their accounts
- Remember to modify the windows built-in firewall
  - Add any exceptions needed for TCP ports

HTTP, FTP and TFTP Services

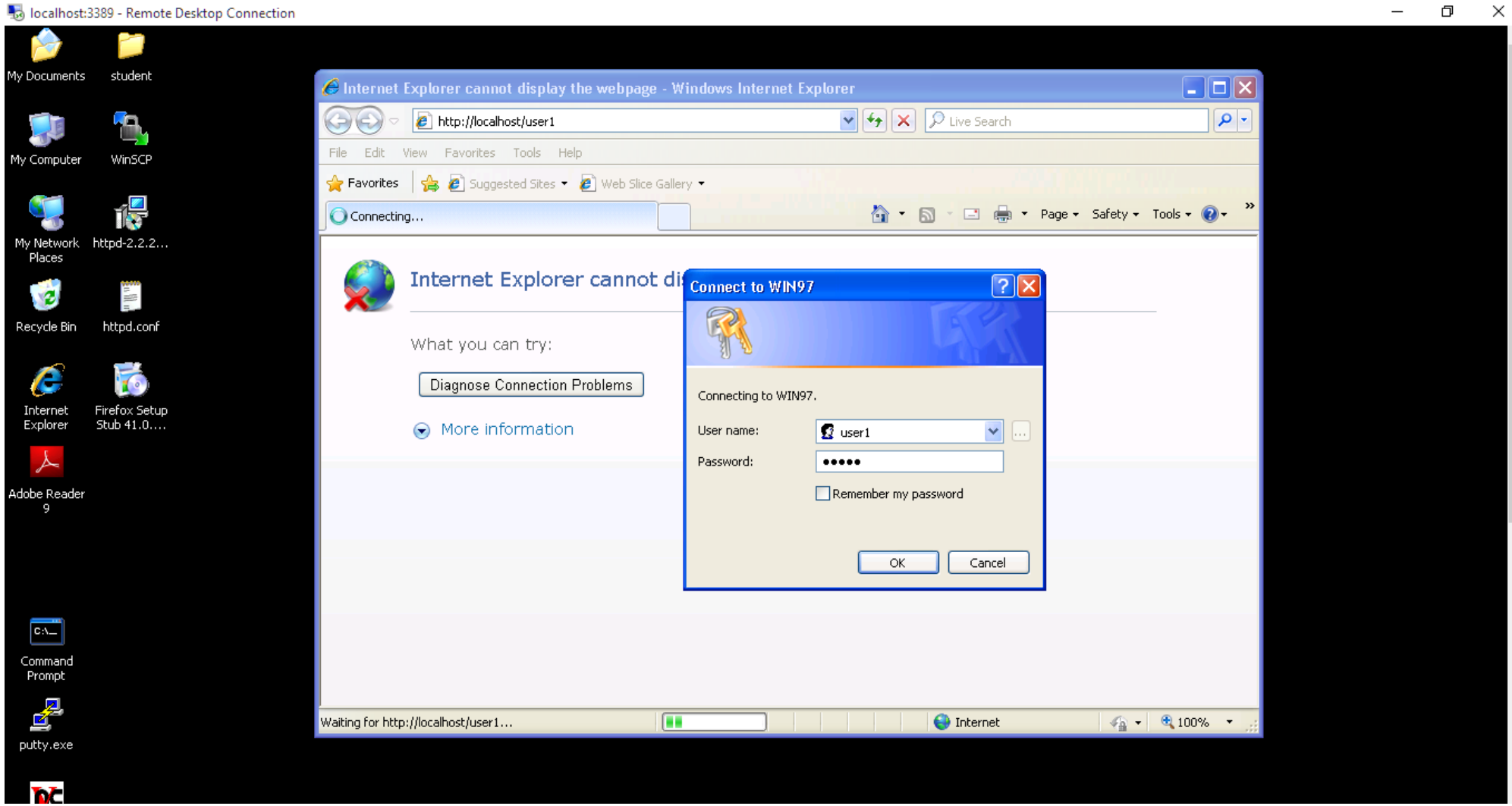
HTTP Service

- Single web page accessible as **webcontent.html at the top level**
- Two sub-directories, each with the name of the regular user you created, **under the top level**
- Access to each of the two subdirectories should only be allowed to the corresponding user
- Again, the user should provides **Windows username/password** credentials

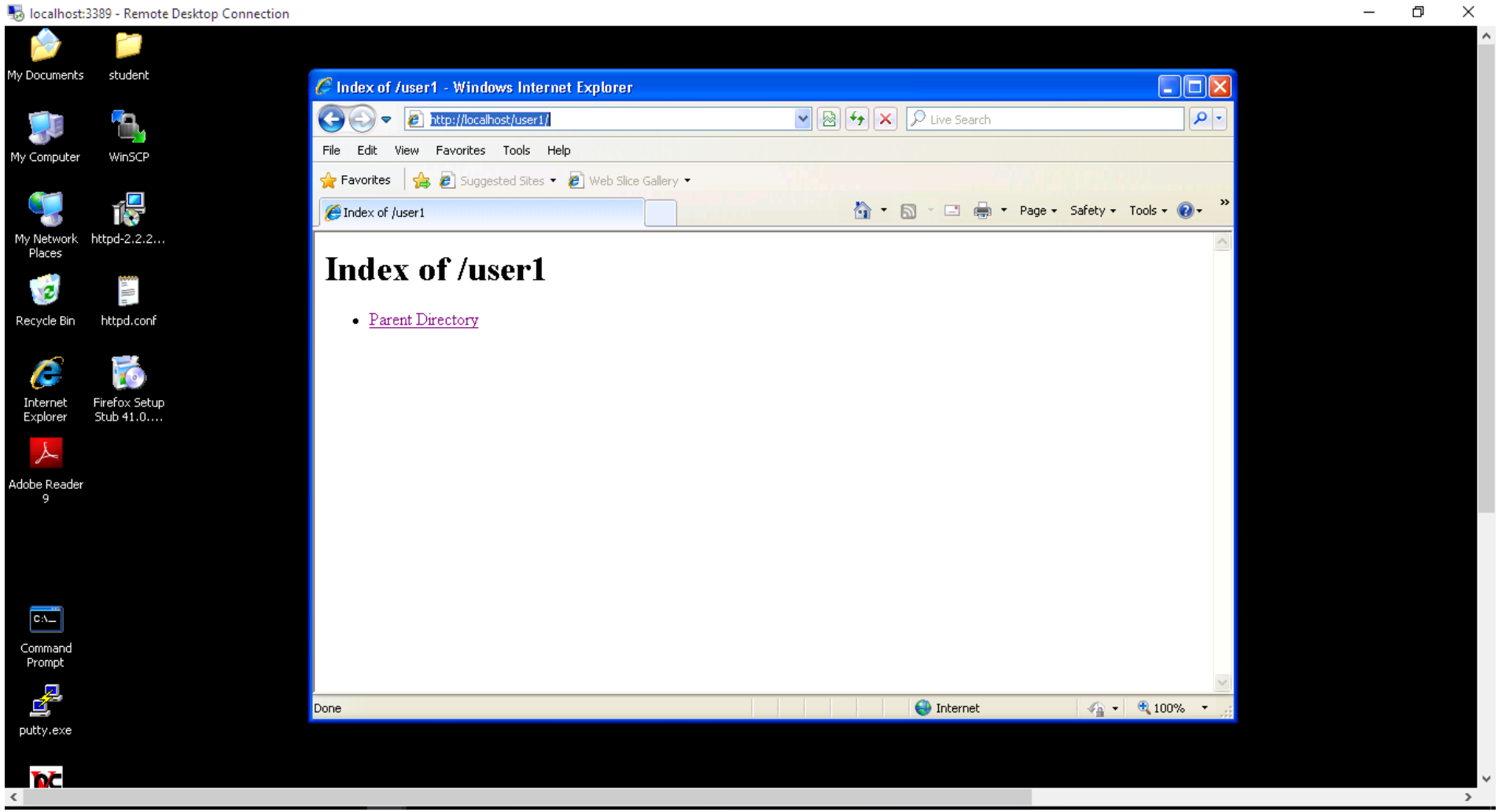
HTTP, FTP and TFTP Services



HTTP, FTP and TFTP Services



HTTP, FTP and TFTP Services



HTTP, FTP and TFTP Services

FTP Service

- Must be on the linux VM
- Recommended software: vsftpd
  - http://ftp.lip6.fr/pub/linux/distributions/slackware/slackware-11.0/slackware/n/vsftpd-2.0.5-i486-1.tgz
  - Install using the "installpkg" command
- Review the connection flow in active and passive modes
  - http://slacksite.com/other/ftp.html

HTTP, FTP and TFTP Services

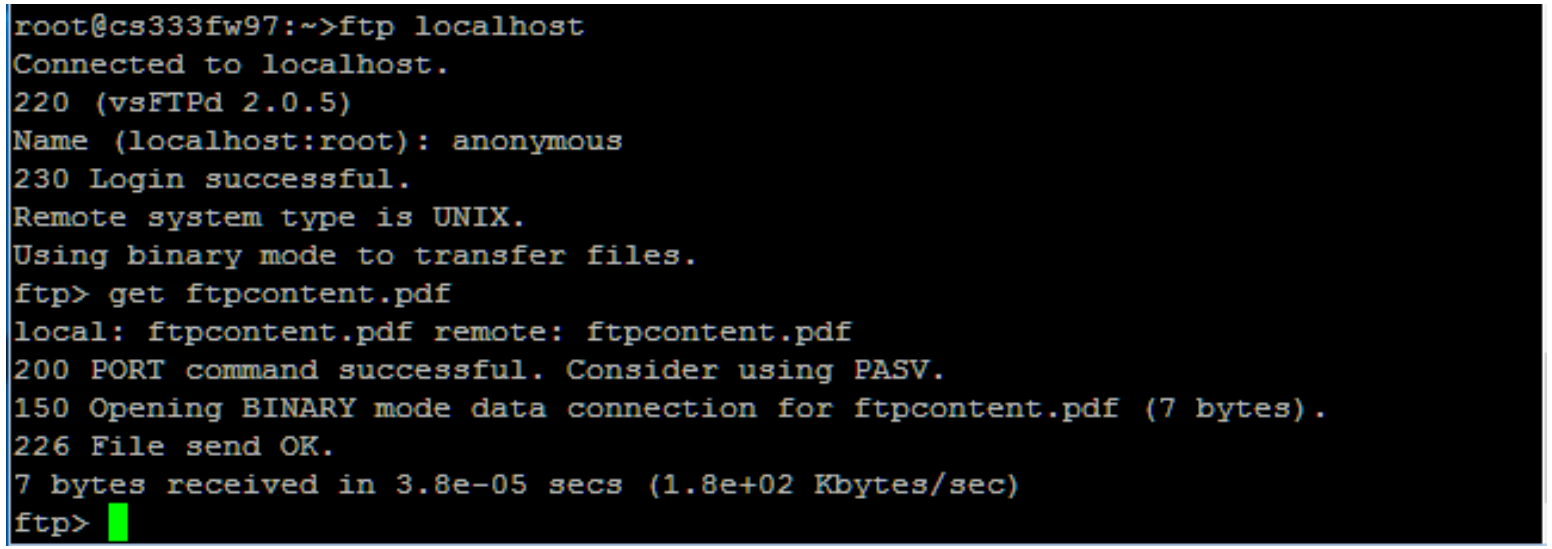
FTP Service

- The ftp service should allow 'anonymous' access as well as access for each user with an account on your Linux host except for **root (root should *not have ftp access)***

```
root@cs333fw97:~>ftp localhost
Connected to localhost.
220 (vsFTPd 2.0.5)
Name (localhost:root): root
530 Permission denied.
Login failed.
ftp>
```

HTTP, FTP and TFTP Services

- **FTP Service – Anonymous access**
  - The ftp server should have at least one file of content available called **ftpcontent.pdf at the top directory** of the space accessed by 'anonymous'.



HTTP, FTP and TFTP Services

- **FTP Service – Anonymous access**
  - An ftp user logging in as anonymous should *not be* allowed to upload files.

HTTP, FTP and TFTP Services

- **FTP Service – User access**
  - The ftp server should allow each regular (non-anonymous) user to upload and download files from a directory. This directory should be different for each regular user.

HTTP, FTP and TFTP Services

TFTP Service

- Must be on the linux VM
- Recommended software: tftpd
  - https://sourceforge.net/projects/tftp-server/

HTTP, FTP and TFTP Services

- **TFTP Service – Access**
  - The tftp server should allow read-only access to the contents of a specific directory (not associated with any user).
  - The directory should have at least one file named **mytftpcontent.pdf**

Firewall

- **Make sure you have enabled netfilter in your kernel**
- **iptables**
  - A tool used to manipulate firewall rules
  - Rules organized in several tables
    - You will be using the default "filter" table which handles local and routed packets
  - Each table has several chains
    - Each has a number of rules which are evaluated in order for each packet that arrives into the chain
    - The first rule to match determines how the packet is handled
    - If no rule matches, the default policy of the chain is applied
    - You can create custom chains

Firewall

The filter table

- **INPUT chain:** handles packets destined for the local machine
- **OUTPUT chain:** handles packets leaving the local machine
- **FORWARD chain:** handles packets being routed
  - Packets to/from your Windows VM will be handled in this chain since they are forwarded by your linux VM's kernel

Firewall

Targets

- Each rule must have a target specifying the decision to be made for packets matching that rule
- ACCEPT target
  - Allows the packet to pass
- DROP and REJECT targets
  - Both block the packet
  - You need to figure out the difference between the two and decide which you want to use
- LOG target
  - Used for logging packets

Firewall

- Bi-directional traffic
  - TCP is a bi-directional protocol and you must have appropriate rules for both directions
  - E.g. if you allow a particular outgoing connection, the inbound traffic for that connection must be allowed as well
- Related traffic
  - Some protocols, such as FTP, may use secondary connections, which should be allowed for proper operation
- iptables "state" module
  - Part of the netfilter connection tracking system
  - Can help you with both of these issues
  - If you use it, make sure that you understand how it works and that you specify in the report how and why you are using it

Firewall

- Further information about iptables
  - A very basic tutorial
  - https://help.ubuntu.com/community/IptablesHowTo
  - A more detailed tutorial
  - Note: Some modules used in the sample rules may not be compiled in your kernel (they are not needed for the assignment)
  - If you are using rules from the tutorials make sure you understand exactly what the rules do and describe in the report how these rules help you achieve your goal
  - The iptables man page

Routing Packets

- For your Windows VM to be able to access the rest of the network you need to have your Linux VM act as a router
  - Change all default passwords on your Windows VM
    - This includes the student account and the VNC password
  - Enable IP forwarding on the Linux VM
    - Check the **/etc/rc.d/rc.ip_forward** script
      - Make it executable if you want it to start on boot
  - Add appropriate rules to the FORWARD chain in iptables

- Questions?