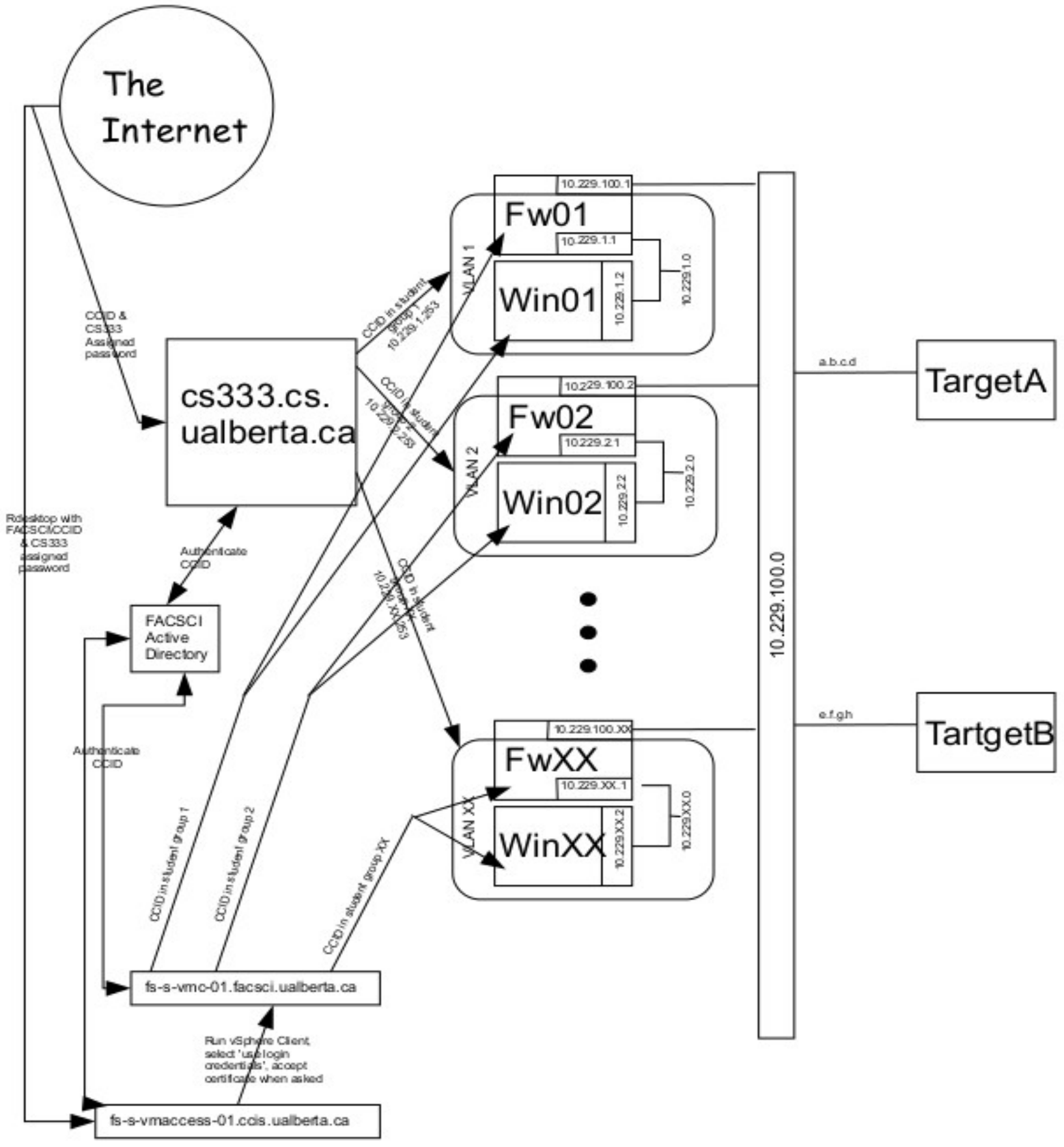
CMPUT 333 - Asn 2

Virtual Lab Presentation


The Internet
cs333.cs.ualberta.ca
CCID & CS333 Assigned password
Rdesktop with FACSCI\CCID & CS333 assigned password
Authenticate CCID
FACSCI Active Directory
Authenticate CCID
fs-s-vmc-01.facsci.ualberta.ca
Run vSphere Client, select 'use login credentials', accept certificate when asked
fs-s-vmaccess-01.ccis.ualberta.ca
CCID in student group 1 10.229.1.253
CCID in student group 2 10.229.2.253
CCID in student group XX 10.229.XX.253
CCID in student group 1
CCID in student group 2
CCID in student group XX
VLAN 1
10.229.100.1
Fw01
10.229.1.1
Win01
10.229.1.2
10.229.1.0
VLAN 2
10.229.100.2
Fw02
10.229.2.1
Win02
10.229.2.2
10.229.2.0
VLAN XX
10.229.100.XX
FwXX
10.229.XX.1
WinXX
10.229.XX.2
10.229.XX.0
10.229.100.0
a.b.c.d
TargetA
e.f.g.h
TartgetB

How to Access VMs

- Access your VLAN (VLANXX where XX is your group) network via the cs333.cs.ualberta.ca server
  - Each VLAN has 2 Virtual Machines
    - WinXX is your Windows VM
    - FwXX is your Linux VM
- Note: Both VM's only have local network access, not Internet access. So if you want to download anything, you'll need to download it on your machine and copy it over using **scp**

How to Access VMs

- Run sshXX script to set up appropriate port forwarding/tunnels

- Download sshXX from eclass and set as executable: **chmod +x sshXX**

- Run: **./sshXX <*group*> <*ccid*>**

- **Use password that was emailed to you, not your CCID password**

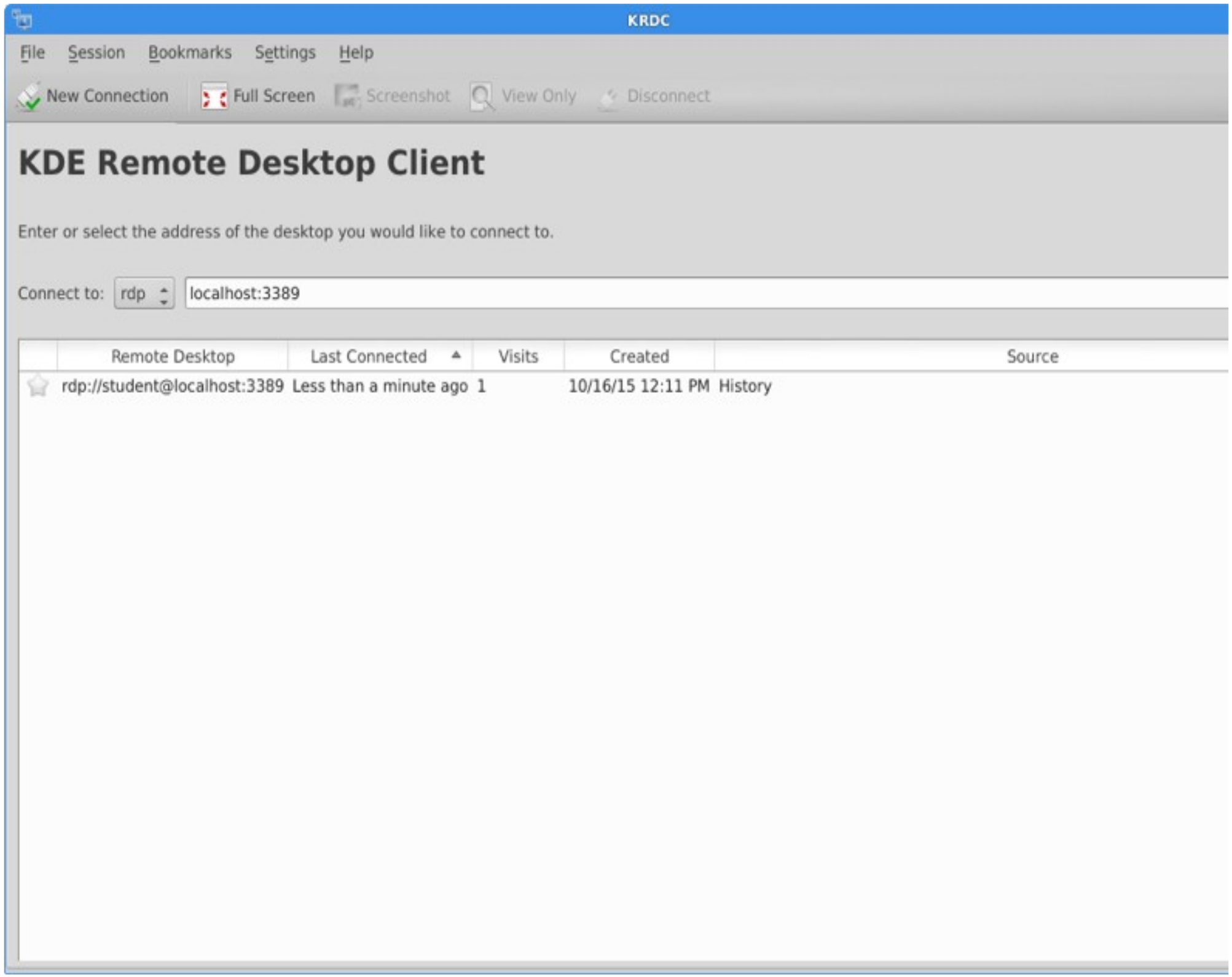
Terminal

File Edit View Terminal Tabs Help

```
hackman@uc07:~/Downloads>ls
sshXX
hackman@uc07:~/Downloads>chmod +x sshXX
hackman@uc07:~/Downloads>ls -l
total 2
-rwx------+ 1 hackman ugrad 1094 Oct 15 13:13 sshXX
hackman@uc07:~/Downloads>./sshXX 95 hackman
Win95:
  rdesktop localhost:3389 -u student
  ssh -p 2222 student@localhost
  vncviewer localhost:5902
  scp -P 2222 file student@localhost:

Fw95:
  ssh -p 2221 root@localhost
  scp -P 2221 file root@localhost:

hackman@cs333.cs.ualberta.ca's password:
Last login: Fri Oct 16 12:08:20 2015 from uc07.cs.ualberta.ca
Cmput333 Firewall (2013)

Hello hackman. You are authenticated from host "129.128.41.17"
This means that until this connection closes, you well be held
responsible for all network activity originating from this host,
to the Computing Science network.

You must leave this connection open while you use this proxy,
although you may iconize, minimize, lower, or otherwise do what
you like to hide this window while you work, as long as you do
not disconnect this session.

DO NOT FORGET to disconnect this session when you are finished.
```

How to Access VMs

- **Must leave sshXX running**
- In another terminal, you can now connect to the VMs.
- To connect to FwXX:
  - **ssh -p 2221 root@localhost**
  - **scp -P 2221 <*filename*> root@localhost:~/** (note scp uses an uppercase P flag, and ssh uses a lower case p flag)
- To connect to WinXX:
  - **ssh -p 2222 student@localhost**
  - **vncviewer localhost:5902**
  - **krdc** (you'll want to use address localhost:3389. Your user id is **student** and your password is **changeme**)
- **Default password for both is "changeme".** Change this. In linux, use **passwd** command.

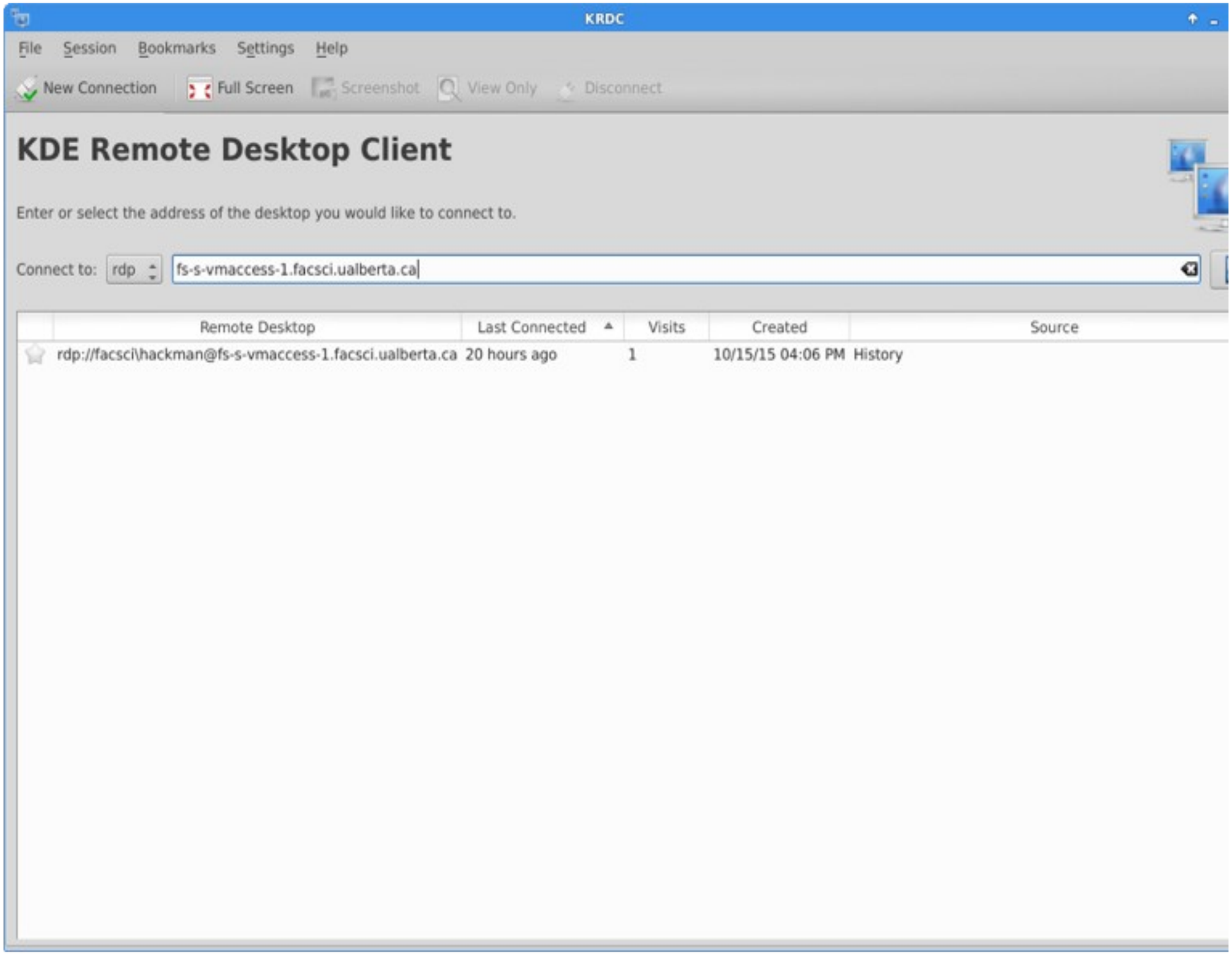

KRDC
File
Session
Bookmarks
Settings
Help
New Connection
Full Screen
Screenshot
View Only
Disconnect
KDE Remote Desktop Client
Enter or select the address of the desktop you would like to connect to.
Connect to:
rdp
localhost:3389
Remote Desktop
Last Connected
Visits
Created
Source
rdp://student@localhost:3389
Less than a minute ago
1
10/16/15 12:11 PM
History

How to connect VM Management Console

Before you begin messing around with the VMs you'll want to take a **snapshot** of the VM which you can restore to if you make any mistakes.

Access VM administrator console by using **krdc** to connect to:

fs-s-vmaccess-1.facsci.ualberta.ca
fs-s-vmaccess-2.facsci.ualberta.ca
fs-s-vmaccess-3.facsci.ualberta.ca


KRDC
File Session Bookmarks Settings Help
New Connection
Full Screen
Screenshot
View Only
Disconnect
KDE Remote Desktop Client
Enter or select the address of the desktop you would like to connect to.
Connect to:
rdp
fs-s-vmaccess-1.facsci.ualberta.ca
Remote Desktop
Last Connected
Visits
Created
Source
rdp://facsci\hackman@fs-s-vmaccess-1.facsci.ualberta.ca
20 hours ago
1
10/15/15 04:06 PM
History

Host Configuration – KRDC

Host Configuration

Connection

Desktop resolution: Normal (1024x768)

Width: 1024 Height: 768

Color depth: High Color (16 Bit)

Keyboard layout: US English (en-us)

Sound: On This Computer

Performance: LAN

RemoteFX: ☑ Enhanced visual experience

Share Media: /media

Expert Options

Console login: ☐ Attach to Windows Server console

Extra options:

☑ Show this dialog again for this host

☐ Remember password (KWallet)

Cancel OK

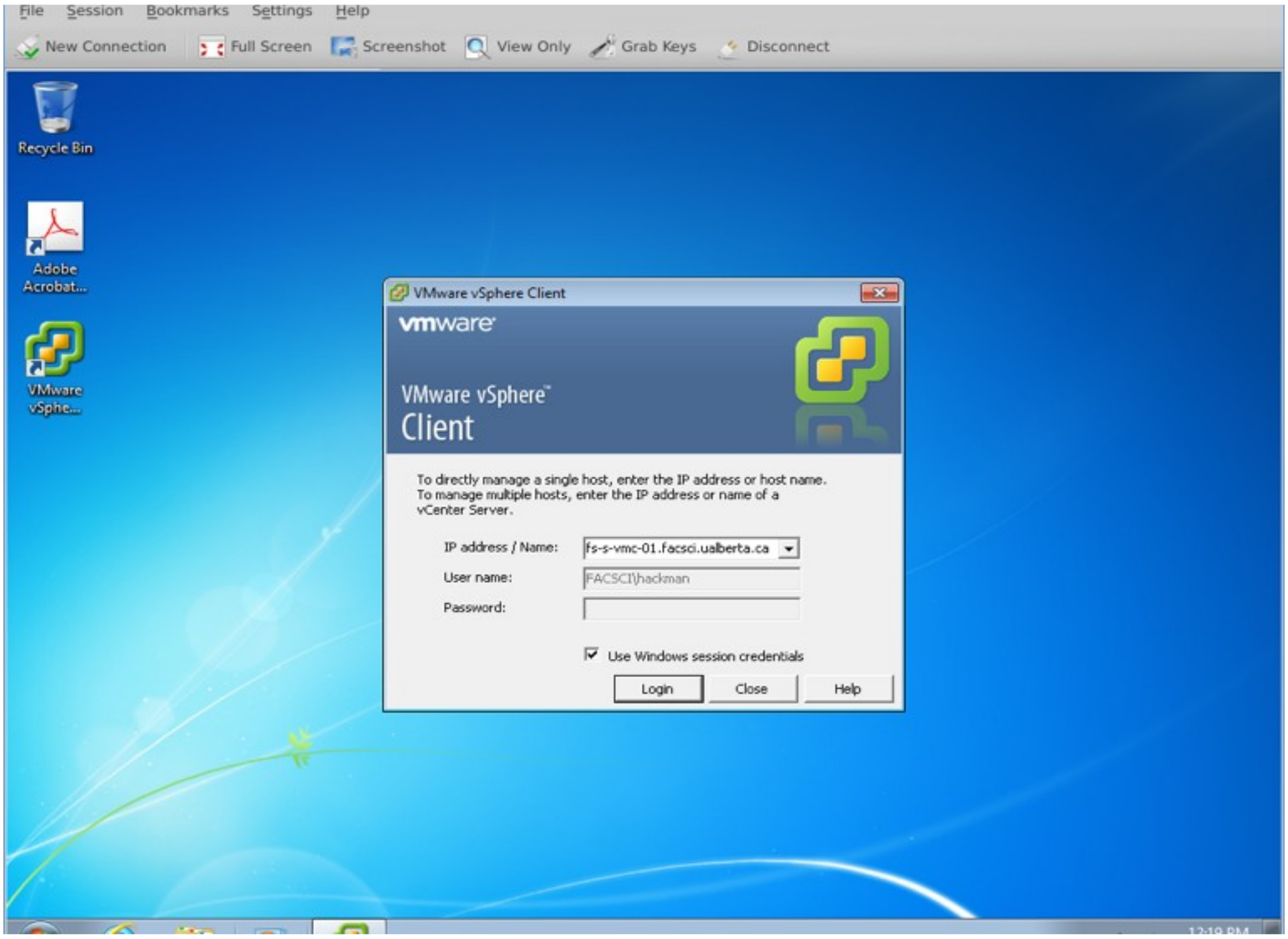

Enter Username - KRDC
Please enter the username you would like to use for login.
facsci\hackman
Cancel
OK

VM Management Console

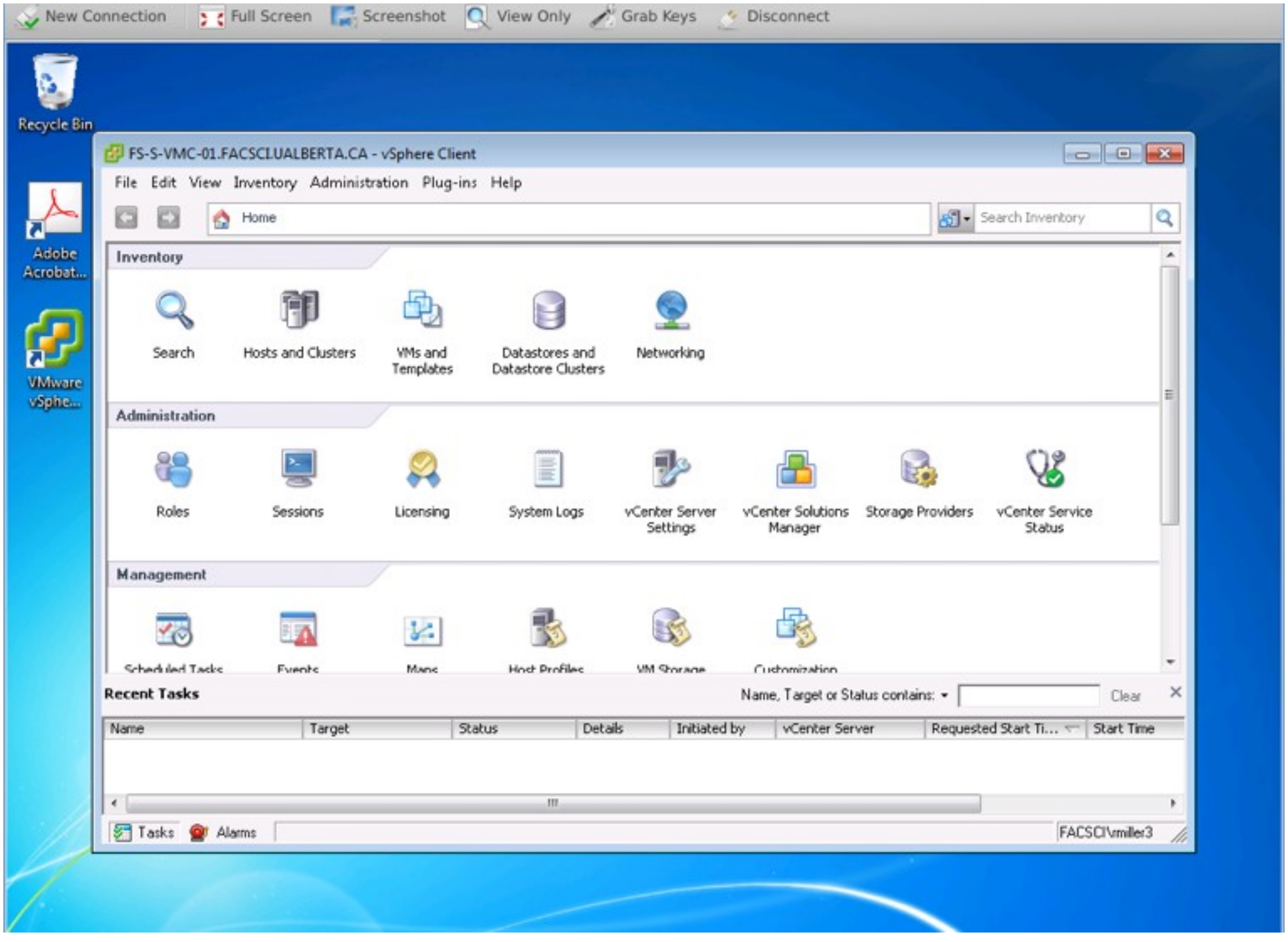
- Use your password to log in.
- Note if you incorrectly enter your password or your name, you krdc will log into a blank blue screen.
- Then open VSphere (should appear on your desktop)
- Use IP Address: fs-s-vmc-01.facsci.ualberta.ca

VM Management Console

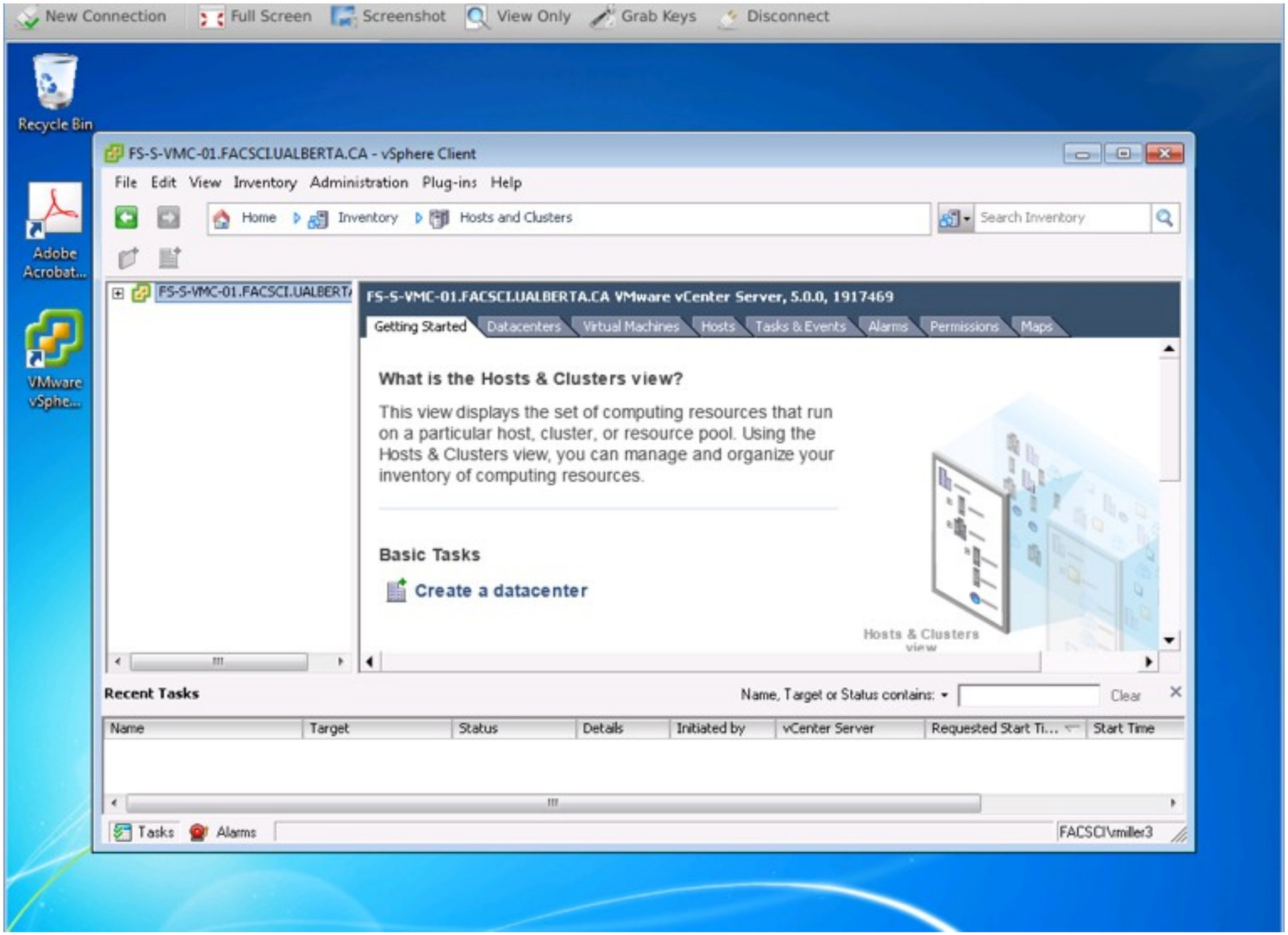
- Use your password to log in.
- Note if you incorrectly enter your password or your name, you krdc will log into a blank blue screen.
- Then open VSphere (should appear on your desktop)
- Use IP Address: fs-s-vmc-01.facsci.ualberta.ca



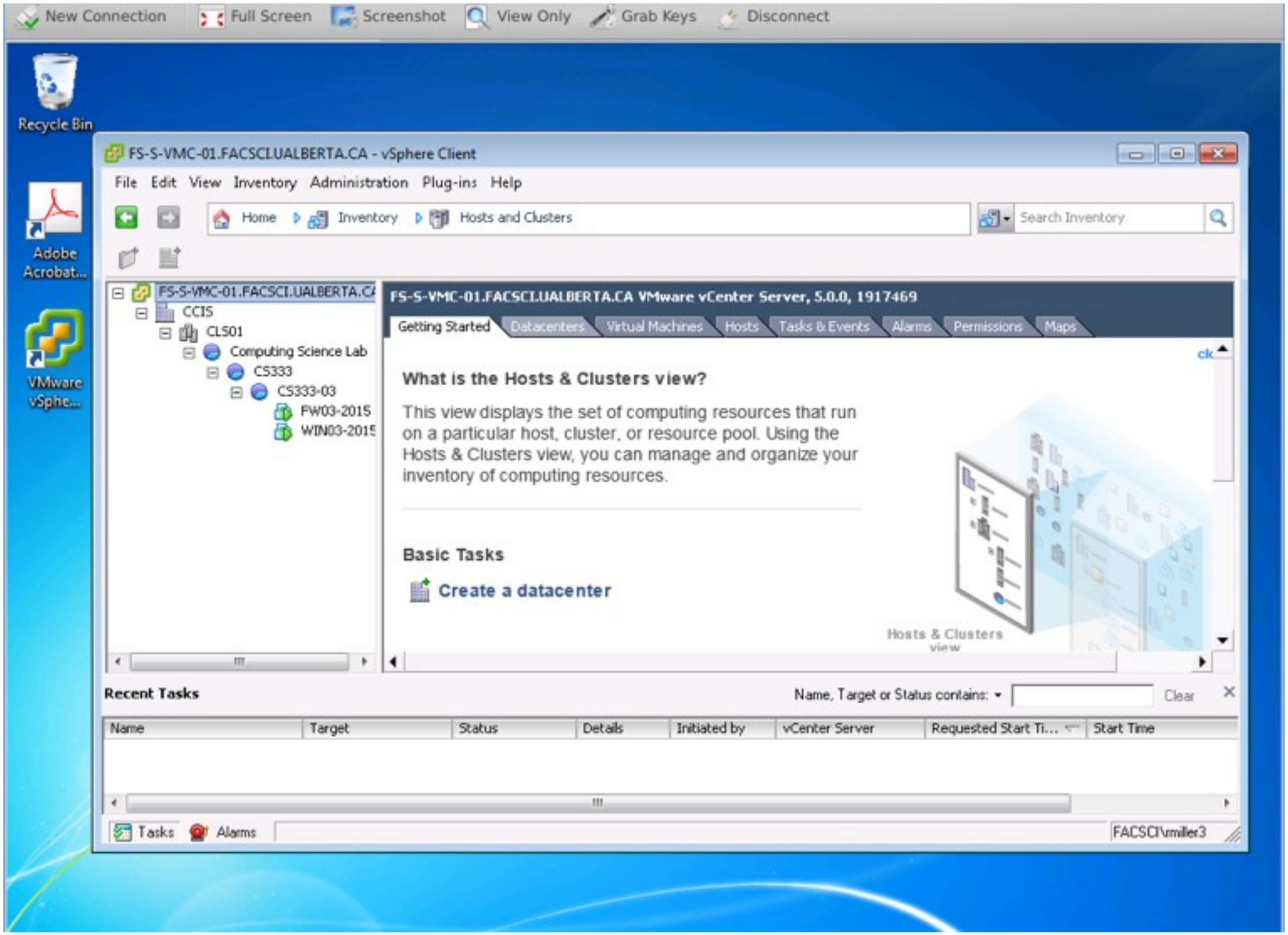
Click the Use Windows Session Credentials to reuse your password & name



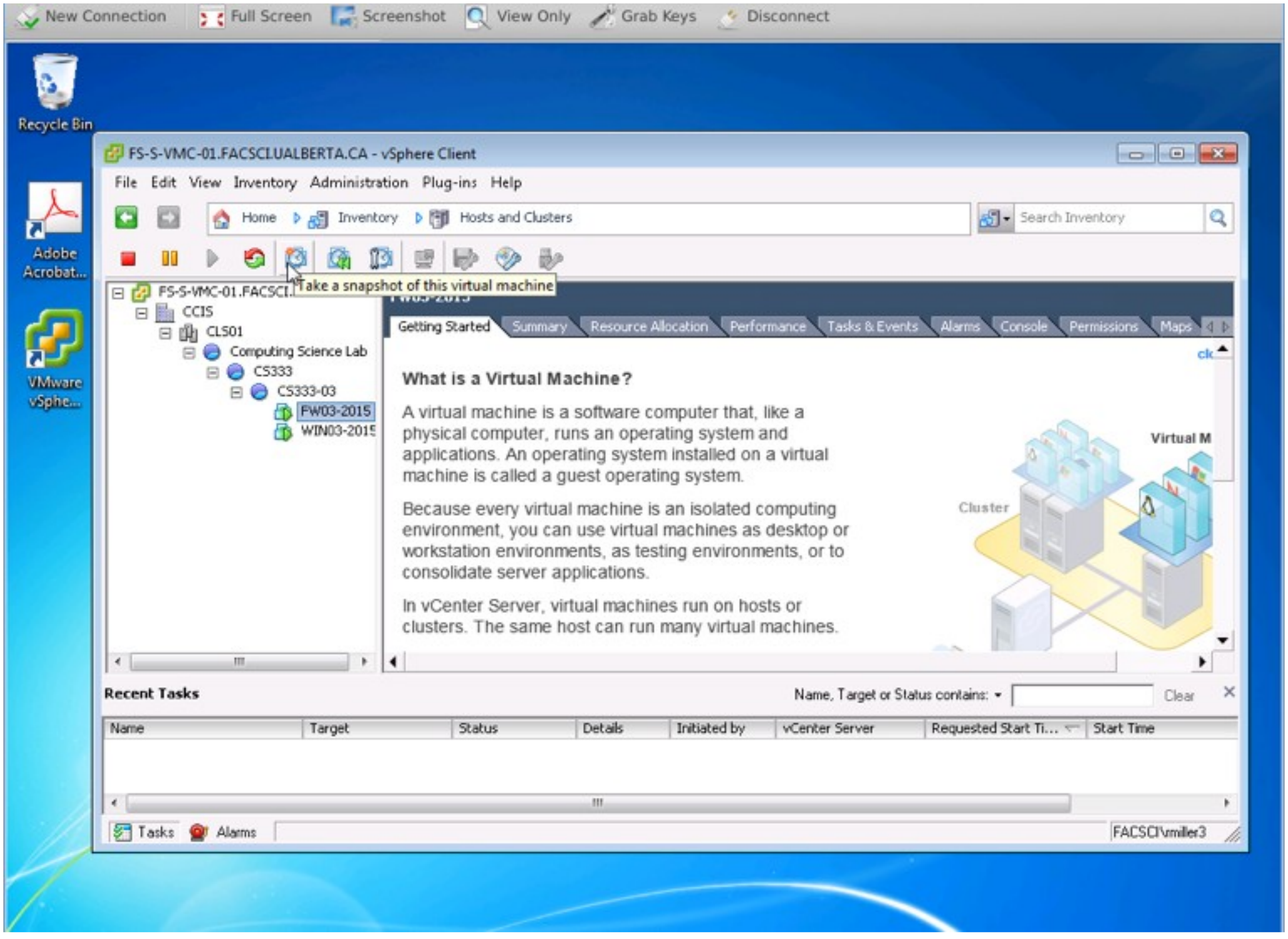
Select “Hosts and Clusters”



Click the + sign beside FS-S-VMC-01.FACSCI.UALBERTA.CA until you drill down to your group VMs



Next, select a VM and take a screenshot!



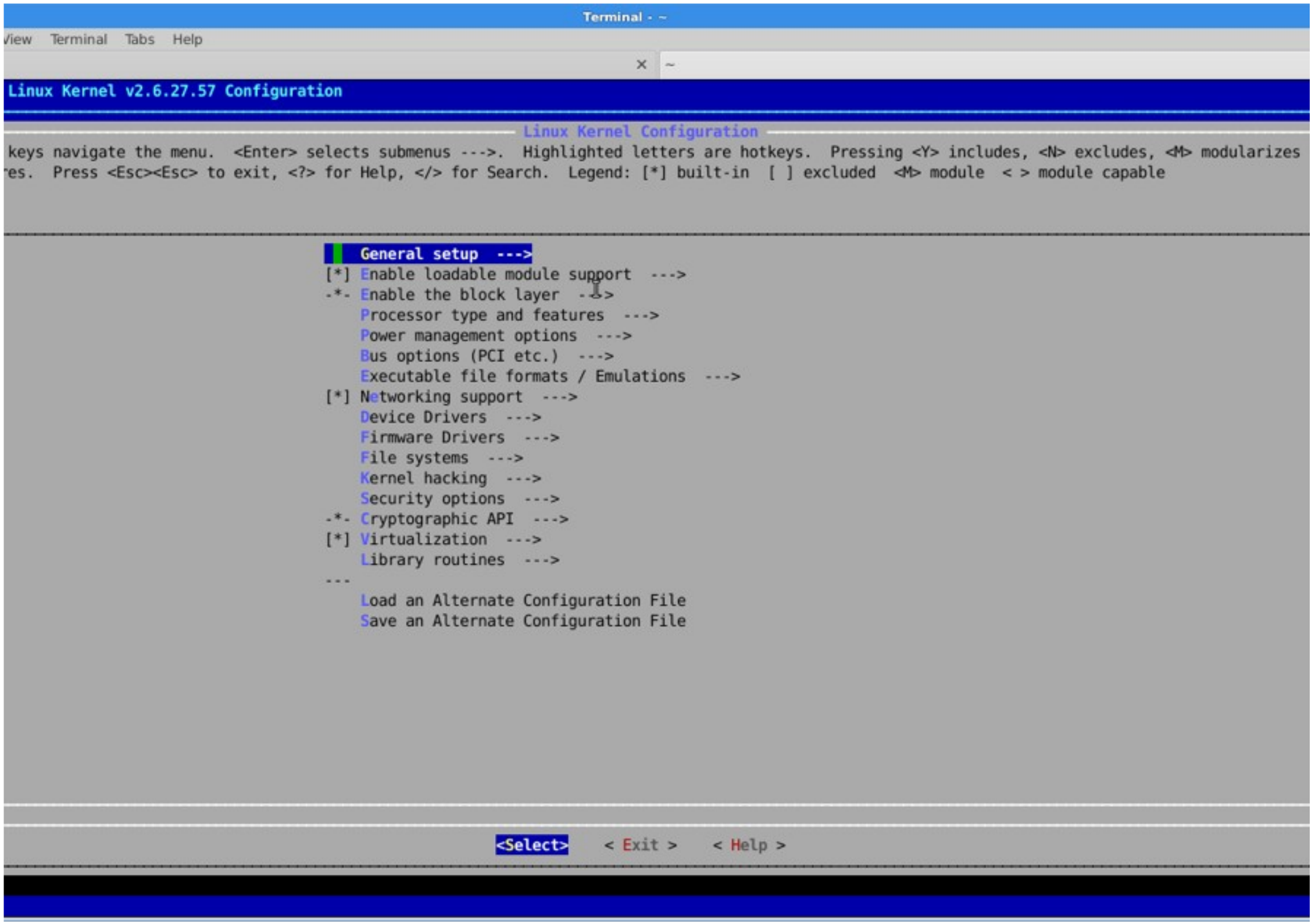
Name your screen shot and a loading bar will appear in recent tasks

Kernel Configuration

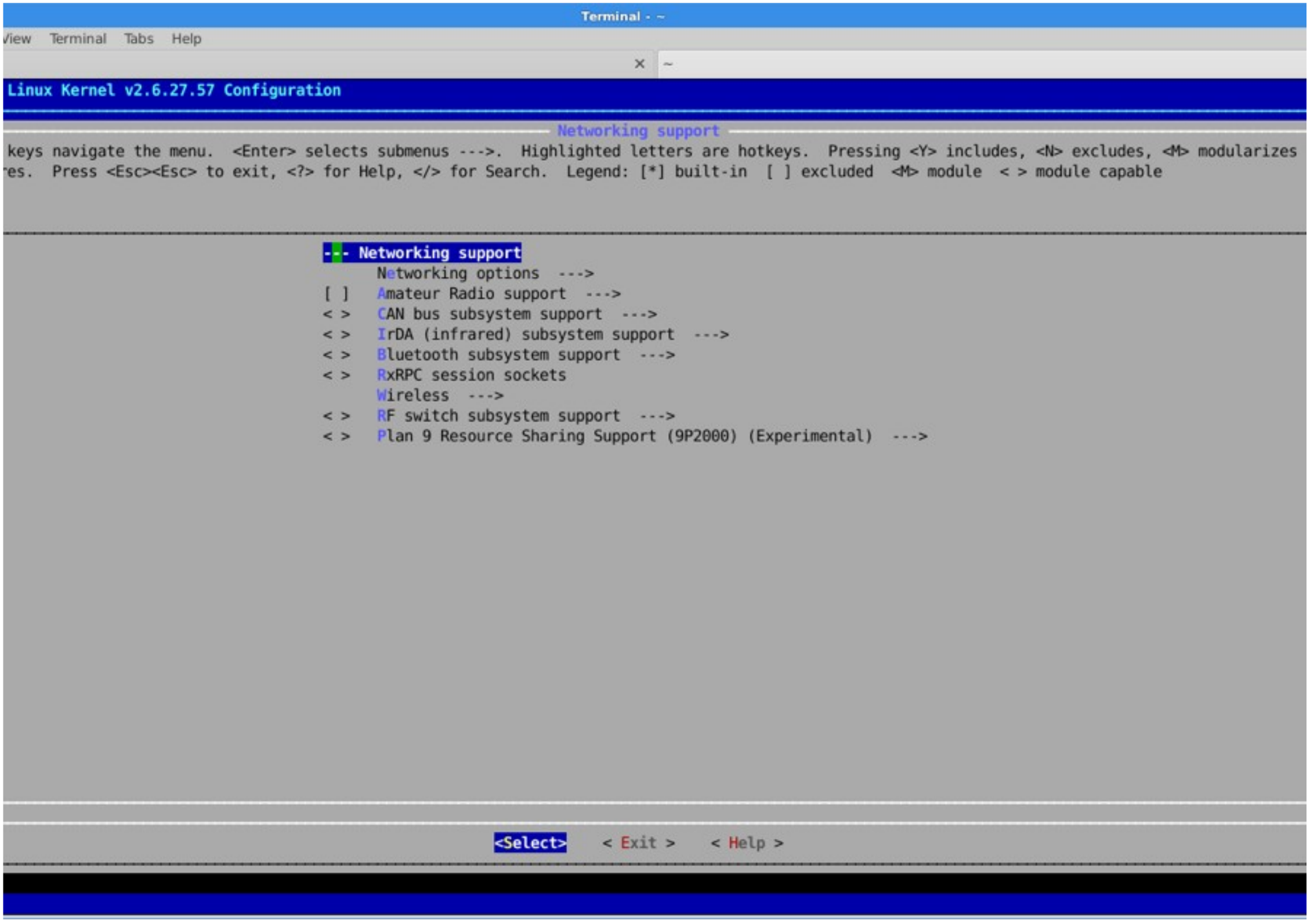
- **TAKE A SNAPSHOT BEFORE YOU START**
- Update the kernel to 2.6.27.57
  - download http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.27.57.tar.bz2 and copy it over to your linux VM
  - extract this in **/usr/src** using **tar -xjvf *filename***
  - Replace the simlink **linux** to point to **linux-2.6.27.57: rm linux & ln -s linux-2.6.27.57 linux**
  - **Double check the symbolic link was established correctly: ls -l**
  - In **/usr/src/linux/include** create a simlink from asm-i386 to asm-x86: **ln -s asm-x86 asm-i386**
  - Copy the .config file from the old kernel **/usr/src/linux-2.6.26** to the new one **/usr/ src/linux**

Kernel Configuration

- Add netfilter support:
  - run **make menuconfig** to reconfigure the kernel
  - **Networking support -> Networking Options-> Network packet filtering framework (Netfilter)**
    - **Core Netfilter Configuration**
      - **Netfilter connection tracking support**
      - **Netfilter Xtables support**
        - **“state” match support**
- **IP: Netfilter Configuration**
  - **IPv4 connection tracking support**
  - **IP tables support**
    - **Packet filtering (IP_NF_FILTER)**
      - **REJECT target support**
    - **LOG target support**


Terminal - ~
View Terminal Tabs Help
~
Linux Kernel v2.6.27.57 Configuration
Linux Kernel Configuration
keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
es. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable
General setup --->
[*] Enable loadable module support --->
-*- Enable the block layer --->
Processor type and features --->
Power management options --->
Bus options (PCI etc.) --->
Executable file formats / Emulations --->
[*] Networking support --->
Device Drivers --->
Firmware Drivers --->
File systems --->
Kernel hacking --->
Security options --->
-*- Cryptographic API --->
[*] Virtualization --->
Library routines --->

Load an Alternate Configuration File
Save an Alternate Configuration File
<Select> < Exit > < Help >


Terminal - ~
View Terminal Tabs Help
~
Linux Kernel v2.6.27.57 Configuration
Networking support
keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
es. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable
--- Networking support
Networking options --->
[ ] Amateur Radio support --->
< > CAN bus subsystem support --->
< > IrDA (infrared) subsystem support --->
< > Bluetooth subsystem support --->
< > RxRPC session sockets
Wireless --->
< > RF switch subsystem support --->
< > Plan 9 Resource Sharing Support (9P2000) (Experimental) --->
<Select> < Exit > < Help >

Terminal - ~

View Terminal Tabs Help

~

Linux Kernel v2.6.27.57 Configuration

Networking options

keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
es. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable

```
<*> Packet socket
[ ]   Packet socket: mmapped IO
<*> Unix domain sockets
< > PF_KEY sockets
[*] TCP/IP networking
[ ]   IP: multicasting
[ ]   IP: advanced router
[ ]   IP: kernel level autoconfiguration
< >   IP: tunneling
< >   IP: GRE tunnels over IP
[ ]   IP: ARP daemon support (EXPERIMENTAL)
[ ]   IP: TCP syncookie support (disabled per default)
< >   IP: AH transformation
< >   IP: ESP transformation
< >   IP: IPComp transformation
< >   IP: IPsec transport mode
< >   IP: IPsec tunnel mode
< >   IP: IPsec BEET mode
<*>   Large Receive Offload (ipv4/tcp)
< >   INET: socket monitoring interface
[ ]   TCP: advanced congestion control  --->
[ ]   TCP: MD5 Signature Option support (RFC2385) (EXPERIMENTAL)
< >   IP virtual server support (EXPERIMENTAL)  --->
< >   The IPv6 protocol  --->
[ ] Security Marking
[*] Network packet filtering framework (Netfilter)  --->
< > The DCCP Protocol (EXPERIMENTAL)  --->
v(+)
```

<Select> < Exit > < Help >

Terminal - ~

View Terminal Tabs Help

~

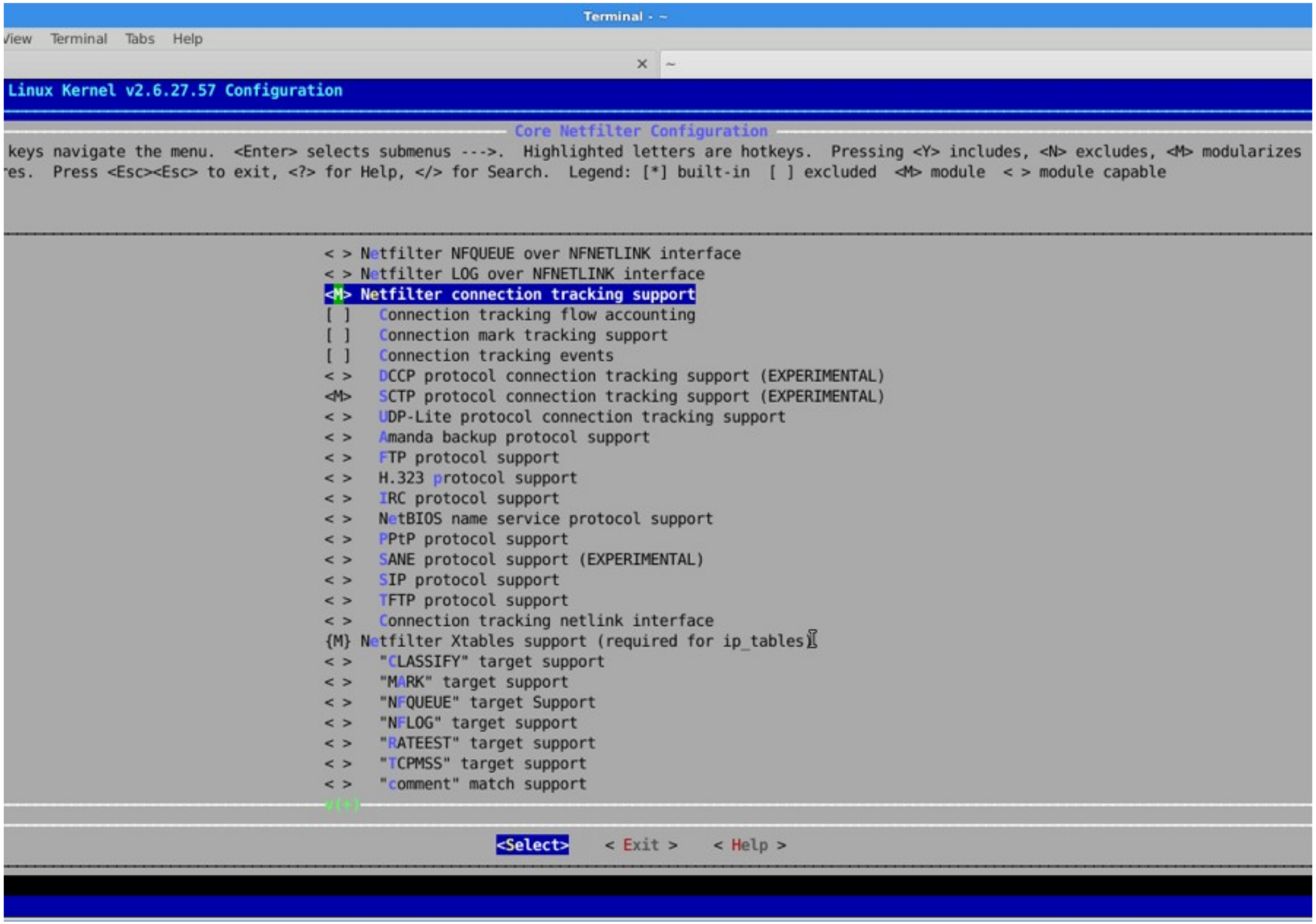
Linux Kernel v2.6.27.57 Configuration

Network packet filtering framework (Netfilter)

keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
es. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable

--- Network packet filtering framework (Netfilter)
[ ] Network packet filtering debugging
[*] Advanced netfilter configuration
Core Netfilter Configuration --->
IP: Netfilter Configuration --->

<Select> < Exit > < Help >


Terminal - ~
View Terminal Tabs Help
~
Linux Kernel v2.6.27.57 Configuration
Core Netfilter Configuration
keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
es. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable
< > Netfilter NFQUEUE over NFNETLINK interface
< > Netfilter LOG over NFNETLINK interface
<M> Netfilter connection tracking support
[ ] Connection tracking flow accounting
[ ] Connection mark tracking support
[ ] Connection tracking events
< > DCCP protocol connection tracking support (EXPERIMENTAL)
<M> SCTP protocol connection tracking support (EXPERIMENTAL)
< > UDP-Lite protocol connection tracking support
< > Amanda backup protocol support
< > FTP protocol support
< > H.323 protocol support
< > IRC protocol support
< > NetBIOS name service protocol support
< > PPtP protocol support
< > SANE protocol support (EXPERIMENTAL)
< > SIP protocol support
< > TFTP protocol support
< > Connection tracking netlink interface
{M} Netfilter Xtables support (required for ip_tables)
< > "CLASSIFY" target support
< > "MARK" target support
< > "NFQUEUE" target Support
< > "NFLOG" target support
< > "RATEEST" target support
< > "TCPMSS" target support
< > "comment" match support
v(+)
<Select> < Exit > < Help >

Terminal - ~

View Terminal Tabs Help

~

Linux Kernel v2.6.27.57 Configuration

Core Netfilter Configuration

keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
es. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable

```
                                    < >   FTP protocol support
                                    < >   H.323 protocol support
                                    < >   IRC protocol support
                                    < >   NetBIOS name service protocol support
                                    < >   PPtP protocol support
                                    < >   SANE protocol support (EXPERIMENTAL)
                                    < >   SIP protocol support
                                    < >   TFTP protocol support
                                    < >   Connection tracking netlink interface
                                    {M} Netfilter Xtables support (required for ip_tables)
                                    < >   "CLASSIFY" target support
                                    < >   "MARK" target support
                                    < >   "NFQUEUE" target Support
                                    < >   "NFLOG" target support
                                    < >   "RATEEST" target support
                                    < >   "TCPMSS" target support
                                    < >   "comment" match support
                                    < >   "connbytes" per-connection counter match support
                                    < >   "connlimit" match support"
                                    < >   "connmark" connection mark match support
                                    < >   "conntrack" connection tracking match support
                                    < >   "dccp" protocol match support
                                    < >   "dscp" and "tos" match support
                                    < >   "esp" match support
                                    < >   "helper" match support
                                    < >   "iprange" address range match support
                                    < >   "length" match support
```

<Select> < Exit > < Help >

Terminal - ~

View Terminal Tabs Help

~

Linux Kernel v2.6.27.57 Configuration

Core Netfilter Configuration

keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
es. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable

```
                    < >   "NFLOG" target support
                    < >   "RATEEST" target support
                    < >   "TCPMSS" target support
                    < >   "comment" match support
                    < >   "connbytes" per-connection counter match support
                    < >   "connlimit" match support"
                    < >   "connmark" connection mark match support
                    < >   "conntrack" connection tracking match support
                    < >   "dccp" protocol match support
                    < >   "dscp" and "tos" match support
                    < >   "esp" match support
                    < >   "helper" match support
                    < >   "iprange" address range match support
                    < >   "length" match support
                    < >   "limit" match support
                    < >   "mac" address match support
                    < >   "mark" match support
                    < >   "owner" match support
                    < >   "multiport" Multiple port match support
                    < >   "pkttype" packet type match support
                    < >   "quota" match support
                    < >   "rateest" match support
                    < >   "realm" match support
                    <M>   "sctp" protocol match support (EXPERIMENTAL)
                    <M>   "state" match support
                    <M>   "statistic" match support
                    < >   "string" match support
```

<Select> < Exit > < Help >

Terminal - ~

View Terminal Tabs Help

~

Linux Kernel v2.6.27.57 Configuration

IP: Netfilter Configuration

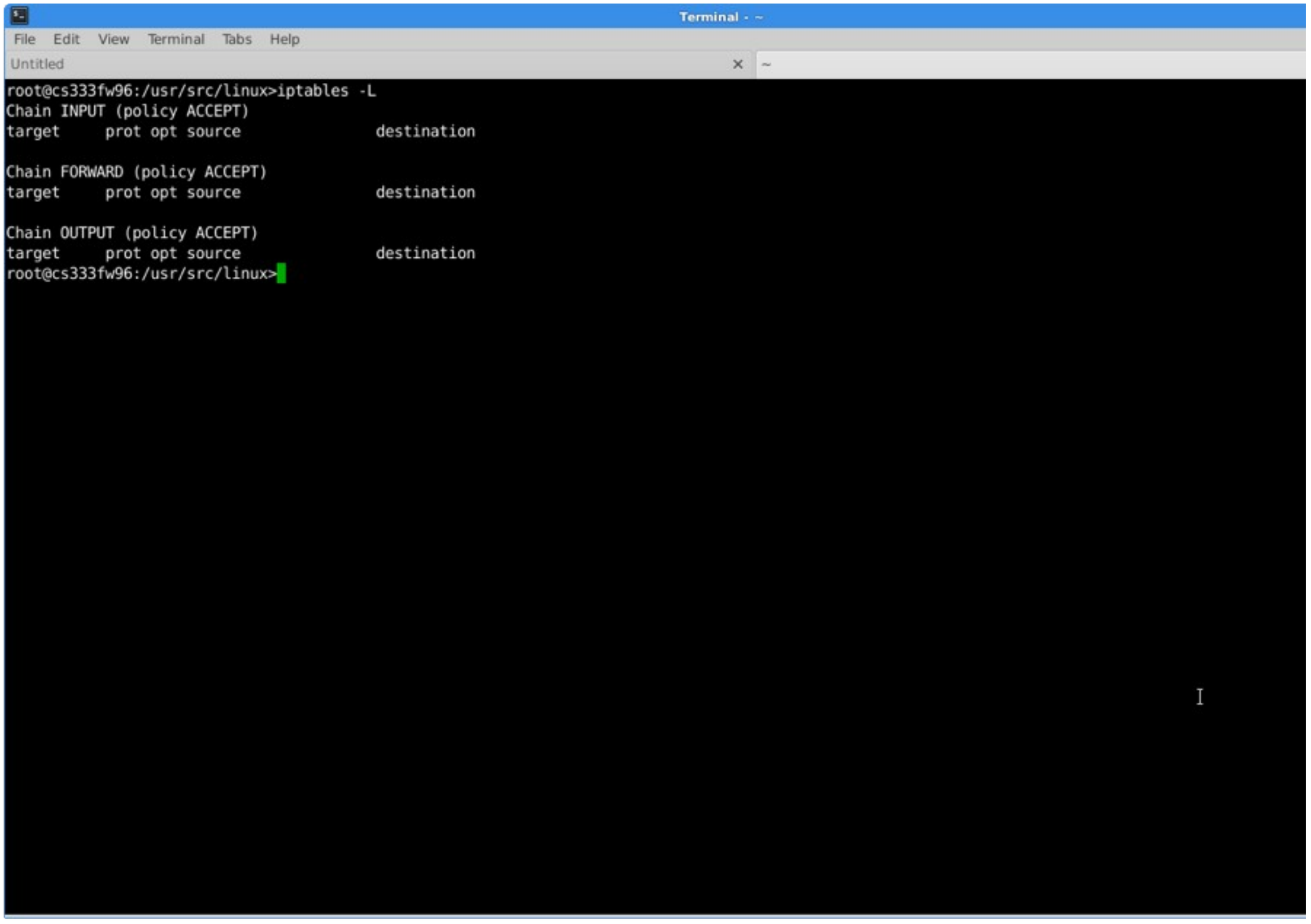
keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes
es. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable

<M> IPv4 connection tracking support (required for NAT)
[*] proc/sysctl compatibility with old connection tracking
< > IP Userspace queueing via NETLINK (OBSOLETE)
<M> IP tables support (required for filtering/masq/NAT)
< > "recent" match support
< > "ecn" match support
< > "ah" match support
< > "ttl" match support
< > "addrtype" address type match support
<M> Packet filtering
<M> REJECT target support
<M> LOG target support
< > ULOG target support
< > Full NAT
< > Packet mangling
< > raw table support (required for NOTRACK/TRACE)
< > ARP tables support

<Select> < Exit > < Help >

Kernel Configuration

- Build the new kernel
  - run **make** to compile
  - run **make modules_install** to install new modules
  - **TAKE A SNAPSHOT**
  - run **make install** to install the new kernel image
- Reboot the VM by running command **reboot**
- Now you should be able to use iptables to confiture your firewall. Try running **iptables -L**


Terminal - ~
File Edit View Terminal Tabs Help
Untitled
~
root@cs333fw96:/usr/src/linux>iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@cs333fw96:/usr/src/linux>