INFO6003 Lab-10 initctl and sudo

Preparation

- We will be using all the VMs from the previous labs
  - Server 2008R2 (password should be Windows1 or Windows12)
    - If prompted to change your password make it Windows!2
  - Windows 7 (password should be Windows1 for **.\User-Admin**)
    - If prompted to change your password make it Windows!2
  - Ubuntu (password should be Ubuntu1 for root and FOLusername users)

Create a LAN Segment

- Under VM settings for one of your VMs go to your Network Adapter and select **LAN Segment**.
- You will need to click on the **LAN Segments…** button to create a new LAN segment.
  - Simply choose **Add** and create a LAN segment called **INFO6003**
- Put all your VMs (both NICs on W7) on the INFO6030 LAN Segment by choosing the LAN Segment in the drop down menu, then power on your VMs. (If they are already powered on, you don't need to power them off to do this)

Configure IPs

- Make sure the IPs of your three VMs are as follows. If you have kept up with the labs your S2008R2 VM will already have this address.

Configuration of Ubuntu VM must be done via the FOLusername-01 account

Server 2008 R2	10.0.0.60	255.255.255.0	
Windows 7	10.0.0.50	255.255.255.0	(must point to Server 2008 R2 for DNS)
Ubuntu Server	10.0.0.20	255.255.255.0	(you will need to use **sudo** to edit this setting)

- For your Linux machine edit the **/etc/network/interfaces** file with your editor of choice. (nano)

Example Settings Below: (use ifconfig to determine your interface, eth?)

```
auto eth?
iface eth? inet static
        address 10.0.0.20
        netmask 255.255.255.0
        network 10.0.0.0
        broadcast 10.0.0.255
```

- Instead of rebooting, we are going to use initctl to restart the interface eth?
- Use **initctl list** to view the running services
  - Which specific service do you think we will want to restart?
  - If you can't find it you can use grep to filter to **network** to make it easier to see.
- You can use the following command to restart a specific interface

initctl restart network-interface INTERFACE=eth#

  - # being your interface ID
  - This command will fail, why did it fail? Fix the command and run it again.

Slide 1: interface successfully restarting and the uname -a output (example on next page)

```
sudo: unable to resolve host ismiley2
network-interface (eth0) start/running
ismiley2-01@ismiley2:~$ uname -a
Linux ismiley2 3.8.0-29-generic #42~precise1-Ubuntu SMP Wed Aug 14 16:19:23 UTC
2013 x86_64 x86_64 x86_64 GNU/Linux
ismiley2-01@ismiley2:~$
```

- Before confirming network connectivity, make sure your Windows VM firewalls are off.

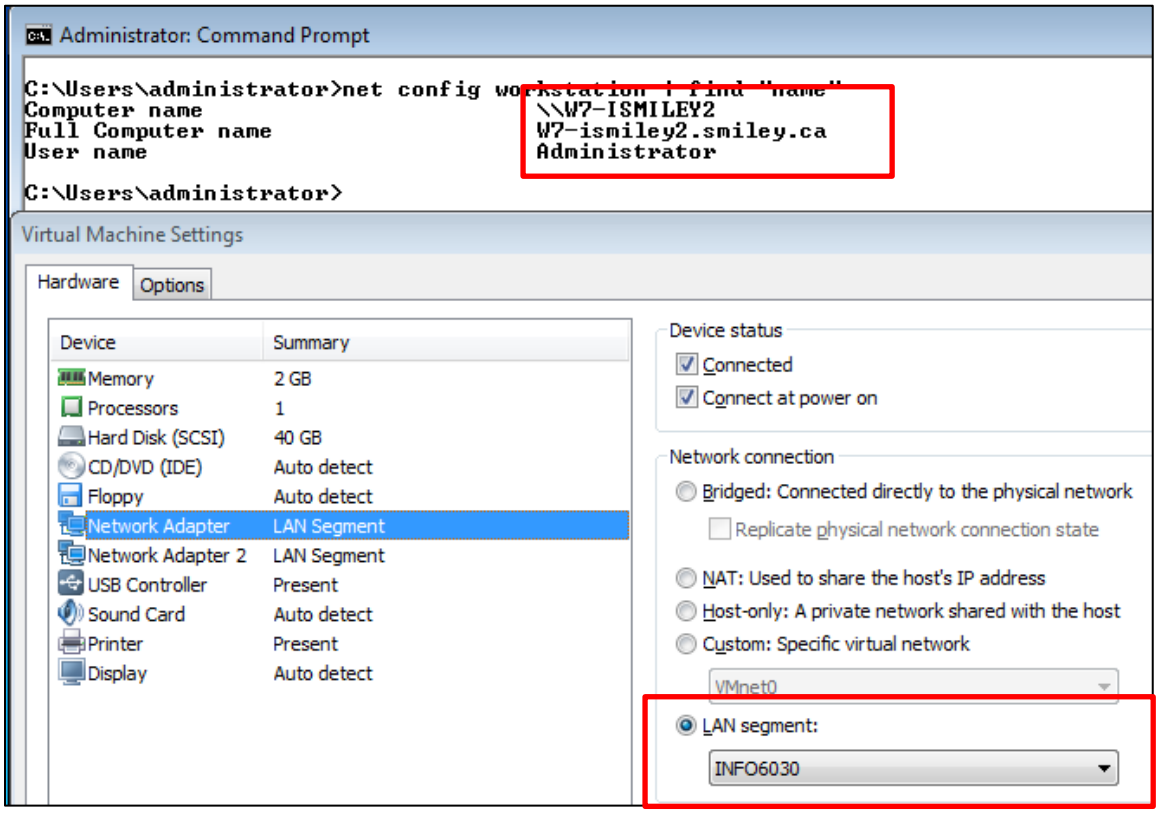
- Use the **ping –c 2 IP address** command to confirm connectivity to your two windows VMs
  - You will use the pipe command and grep to filter your output (similar to find on Windows)

Slide 2: clear the screen with the clear command, then give me the output of two pings filtered to just show lines including ttl (grep usage below) and then issue the uname –a command

```
ismiley2-01@ismiley2:~$ ping -c 2 10.0.0.50  | grep ttl
64 bytes from 10.0.0.50: icmp_req=1 ttl=128 time=0.984 ms
64 bytes from 10.0.0.50: icmp_req=2 ttl=128 time=0.255 ms
ismiley2-01@ismiley2:~$ ping -c 2 10.0.0.60  | grep ttl
64 bytes from 10.0.0.60: icmp_req=1 ttl=128 time=1.06 ms
64 bytes from 10.0.0.60: icmp_req=2 ttl=128 time=0.352 ms
ismiley2-01@ismiley2:~$ uname -a
Linux ismiley2 3.8.0-29-generic #42~precise1-Ubuntu SMP Wed Aug 14 16:19:23 UTC
2013 x86_64 x86_64 x86_64 GNU/Linux
ismiley2-01@ismiley2:~$ _
```

- Logon to your Windows 7 VM as the **domain administrator** before you attempt to gather the information below. (make sure DNS is set correctly if you are having problems)

Slide 3: net config workstation filtered to lines with name, and LAN Segment Setting for W7 VM



SUDO

- Shut your S2008 VM down for this potion
- Disable or disconnect your extra network adapter from the W7 (the one without the static IP)

To demo the sudo command, permission will be granted to the limited user **FOLusername-02** to execute a sniffer utility called tcpdump.

- Ensure that the network is working by pinging your Ubuntu image **from the W7 VM**

- As root, on your Ubuntu VM, verify that tcpdump is working from your home directory.
  - You will need to switch to the root account

root@FOLusername:~#**tcpdump**

- Ping the Ubuntu image from your W7 VM.
- The pings should be captured directly on the screen.

Note: If you don't see anything, or the VM didn't capture what you expected, try running tcpdump with the following option: **tcpdump -n**

- What does the -n do? You can use **man tcpdump** to find out.

- Exit tcpdump by pressing Ctrl + C
- Logout of the Ubuntu VM and **login as user FOLusername-02**. (Don't use su)

- Enter the command **sudo tcpdump** then the appropriate password (might take a while)
  - don't worry about the unable to resolve error

This command should fail because FOLusername-02 doesn't have the appropriate permissions.
  - What does the error tell you?

To grant the user **FOLusername-02** permission to execute tcpdump an entry can be added to the sudoers configuration file. We need to edit the /etc/sudoers file to give the user FOLusername-02 sudo privileges.

- Switch (su) to the root user and use the **visudo** command to edit the sudoers file.
  - Note: the system opens a temp file **etc/sudoers.tmp**

- In the /etc/sudoers file **add** the following lines in the sections listed below:

Cmnd alias specification
Cmnd_Alias SNIFFER = /usr/sbin/tcpdump

#User privilege specification
FOLusername-02 ALL = SNIFFER, /usr/sbin

Save the changes:
- **Ctrl + x**
- **Y**
- Edit the file name to **remove** the **.tmp** and press **Enter**
- File exists, overwrite? **Y**

- **Logout from root** and try running tcpdump via the sudo command as user FOLusername-02.

sudo tcpdump (it could take a while to get the password prompt)

- Ping the Ubuntu server from the W7 VM.
  - It may take a minute for the pings to show up on the Ubuntu VM
  - When the ping is complete, press **Ctrl + c** to end the running capture.

Slide 4: include the tcpdump output (at least one request and reply) and the output of the uname –a command