

Cyber Security Technologies

Session 1b – RADISH

Shawn Davis
ITMS 448 – Spring 2016

Topics

- Part I – PH218 Lab Workstations
- Part II – Accessing Rice Campus Student VMs from PH218 via RADISH
- Part III – Accessing Student VMs from your Personal/Home computer via RADISH
- Part IV – RADISH Rules

Part I

PH218 Lab Workstations

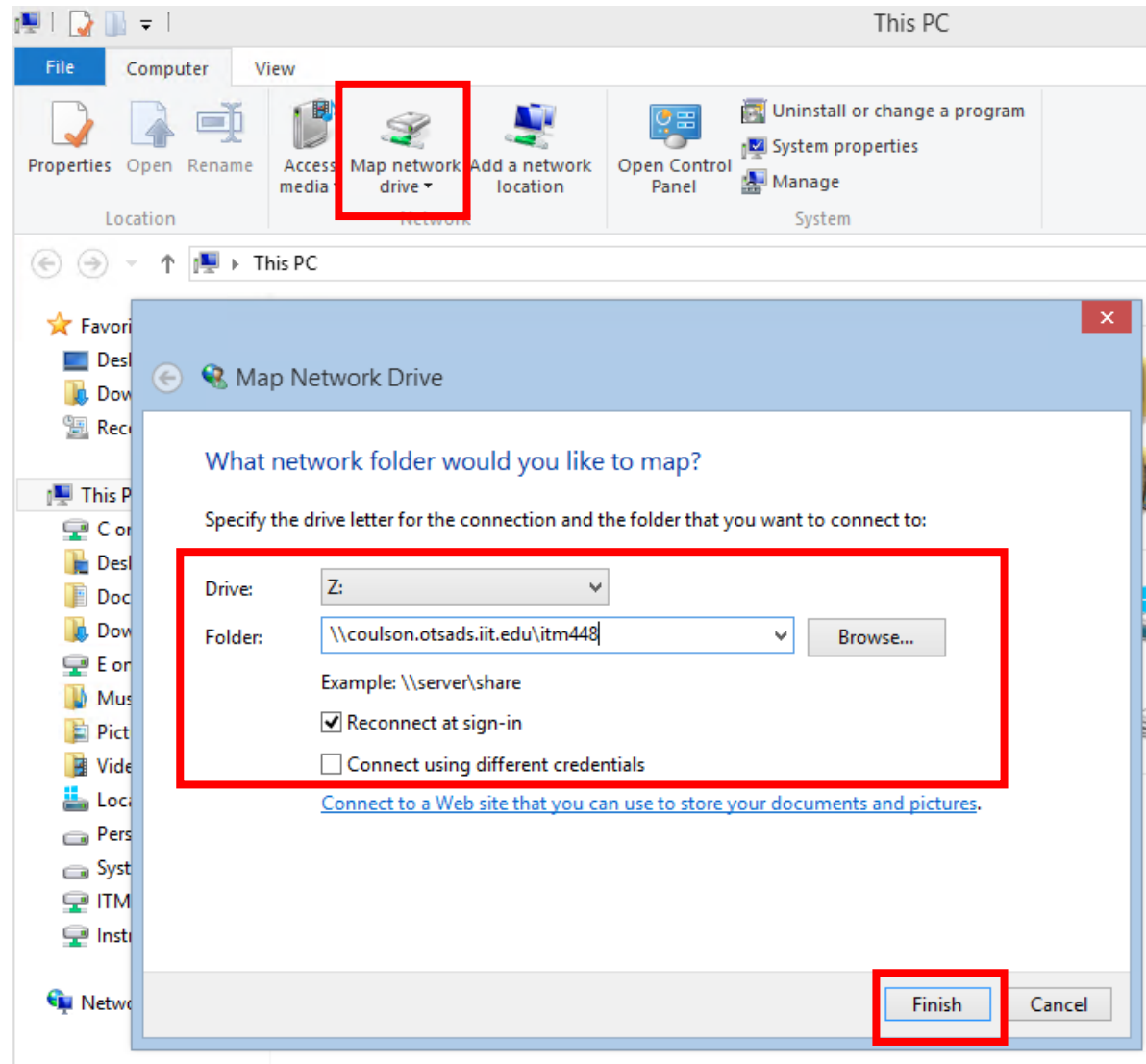
PH218 Lab Workstations

- This is your physical desktop with Win 8.1
- Go ahead and log into your Win 8.1 student workstation with your myIIT student credentials
- You will mainly use this workstation to remote into your ITMS448 student VM at the Rice campus via VMware View Horizon.

PH218 Share

- \\coulson.otsads.iit.edu\itm448
- If not already mapped, go ahead and map it now to a drive letter
- I have put some OVA files (for VirtualBox) on this share
- At times we may use these workstations for exercises without remoting into RADISH

PH218 Share



Part II

Accessing Rice Campus Student VMs from PH218 with RADISH

What is RADISH

- RADISH is our virtual desktop infrastructure that utilizes VMware View to access:
 - Student VM's:
 - Windows 8.1 Virtual Machine (VM)
 - Kali Linux VM via VNC from Windows 8.1 VM
 - We may add others as the semester progresses...

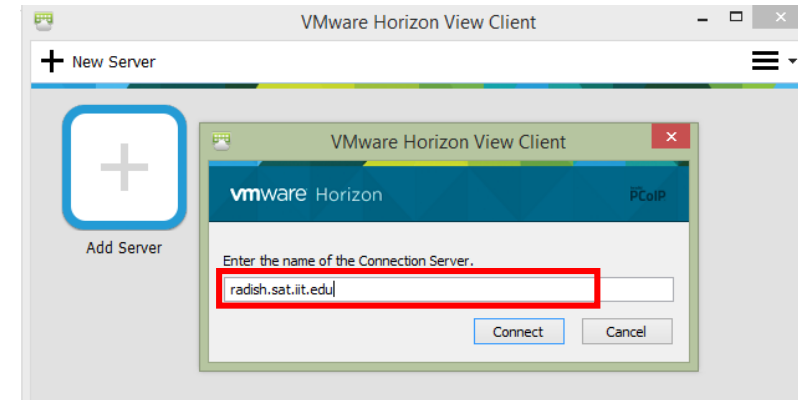
VMware View Client on Lab PCs

- Your PH218 Lab computer is already preinstalled with VMware View Client
- Click on Start > Type **View** (this will start a search)> Run the **VMware Horizon View Client** by clicking on the VMware Horizon View Client icon located on the right side of the start window
- *I suggest placing a shortcut of the Client on your desktop*
- *VMware View is the mechanism by which you will access RADISH on which your VMs are running*

Connecting to RADISH Using VMware View

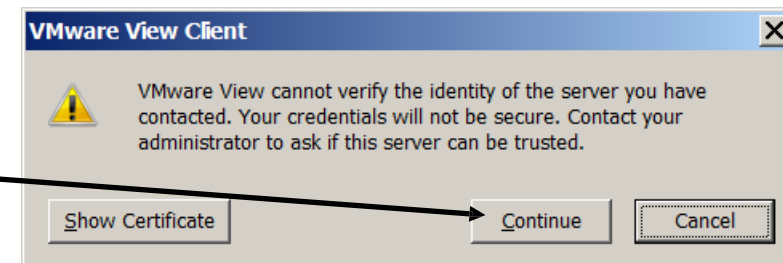
Start the VMware View Client
Set the connection server address
to *radish.sat.iit.edu*

Click on Connect



This screen might pop-up

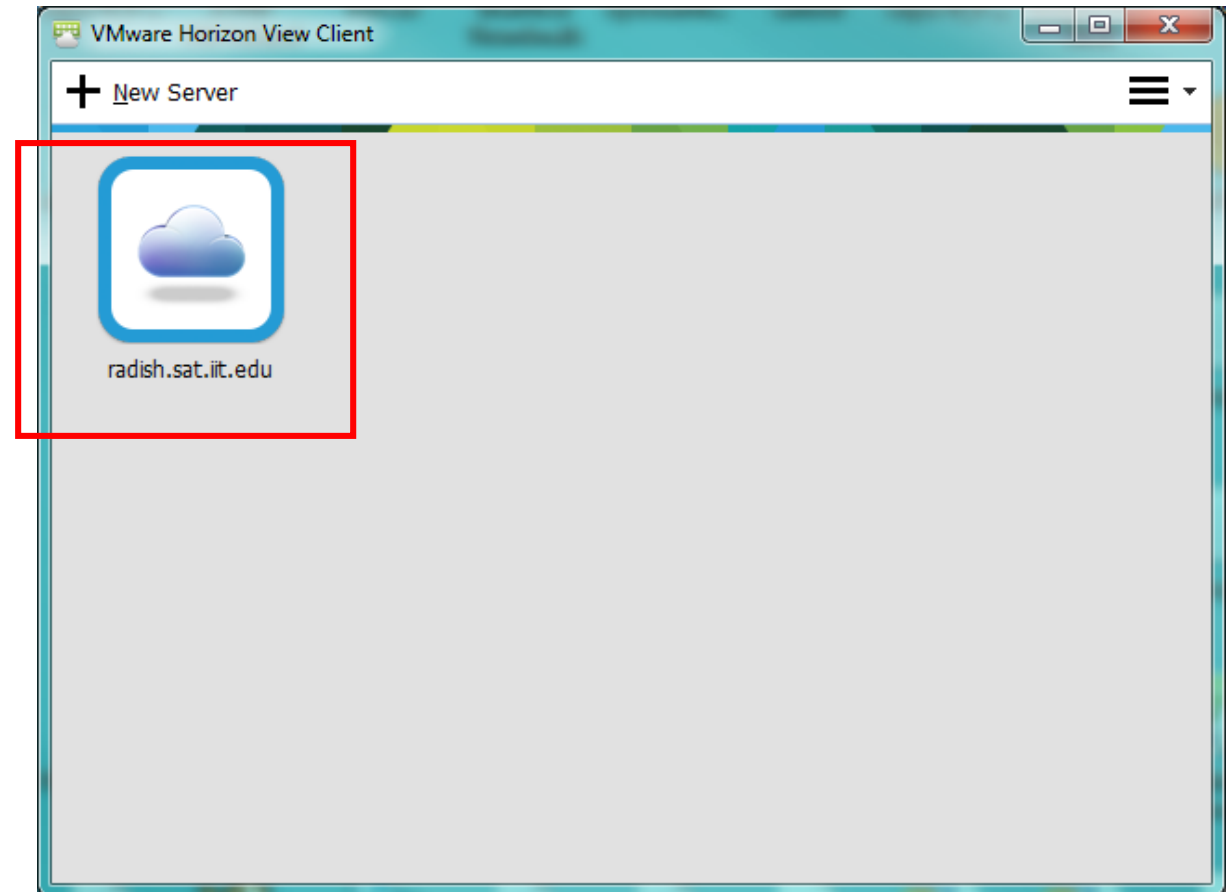
Click on Continue



Note: Your VMware Horizon View Client will look a little different than these slides

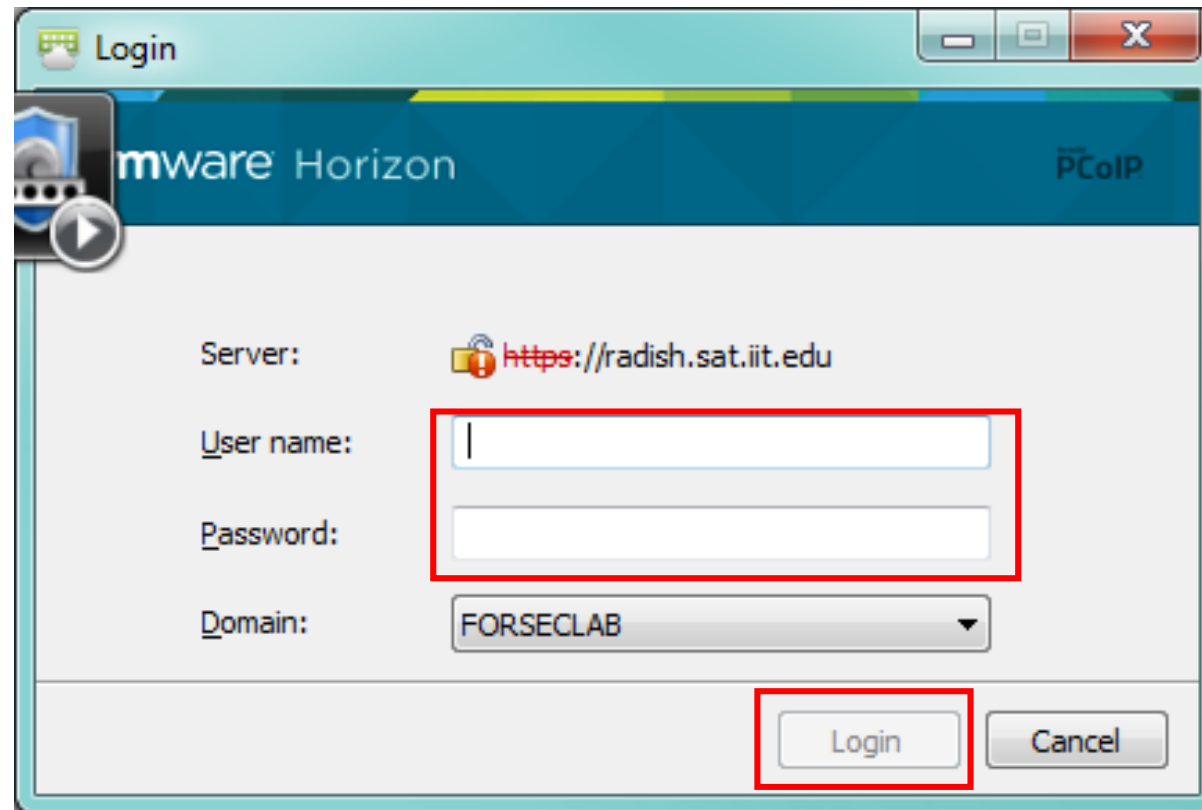
VMware View Client Usage

- Double-click on the Radish server icon



VMware View Client Usage

- Enter your Username and Password that was emailed to you by Dawid this week:



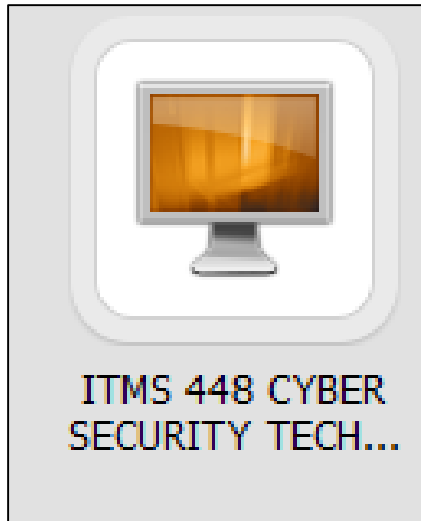
The screenshot shows the VMware Horizon login window. The title bar says "Login". The main header is "vmware Horizon" with "PCoIP" on the right. The login form includes the following fields:

- Server:** <https://radish.sat.iit.edu>
- User name:** A text input field with a red border.
- Password:** A text input field with a red border.
- Domain:** A dropdown menu showing "FORSECLAB".

At the bottom right, there are two buttons: "Login" (highlighted with a red border) and "Cancel".

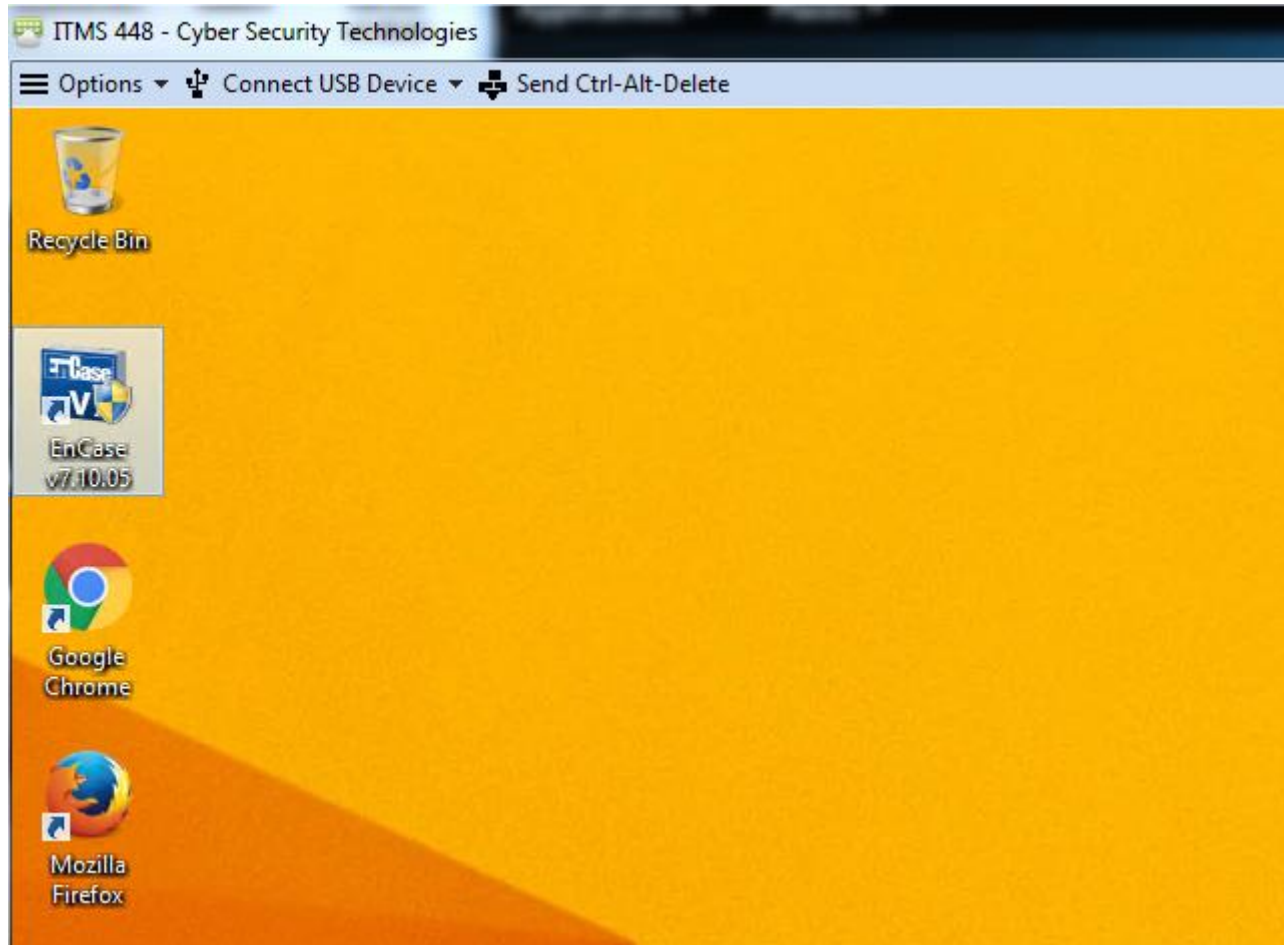
VMware View Client Usage

- Double-click on your ITMS 448 Cyber Security Technologies VM



- Your VM desktop should then load

Win 8.1 VM

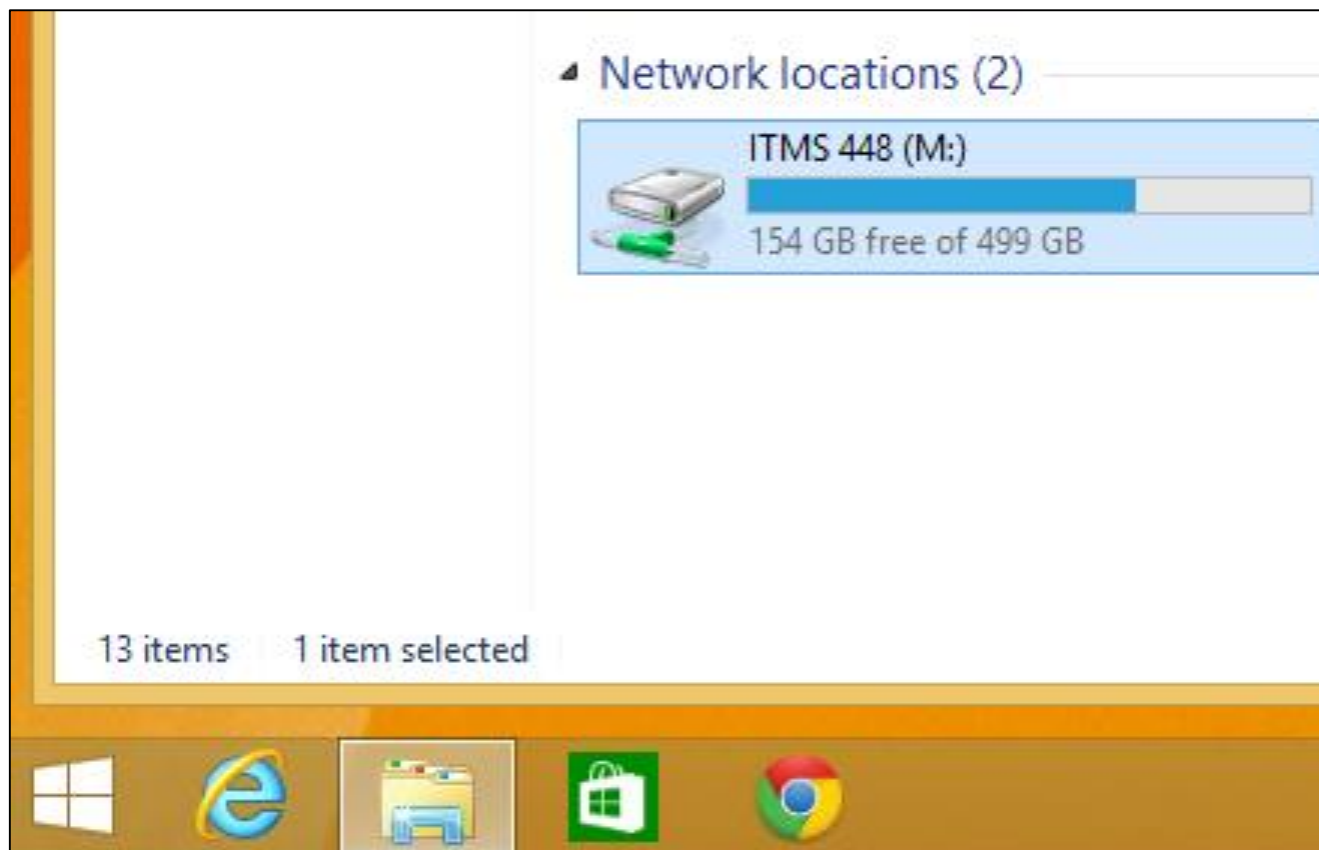


Win 8.1 VM Notes

- Don't ever shut down this VM. To exit, just click the X in the upper right
- Don't change your screen resolution
- If you ever need admin access to install class software to your RADISH Win 8.1 VM, you can use the following credentials for the UAC:
 - Username: **.\student**
 - Password: **student**

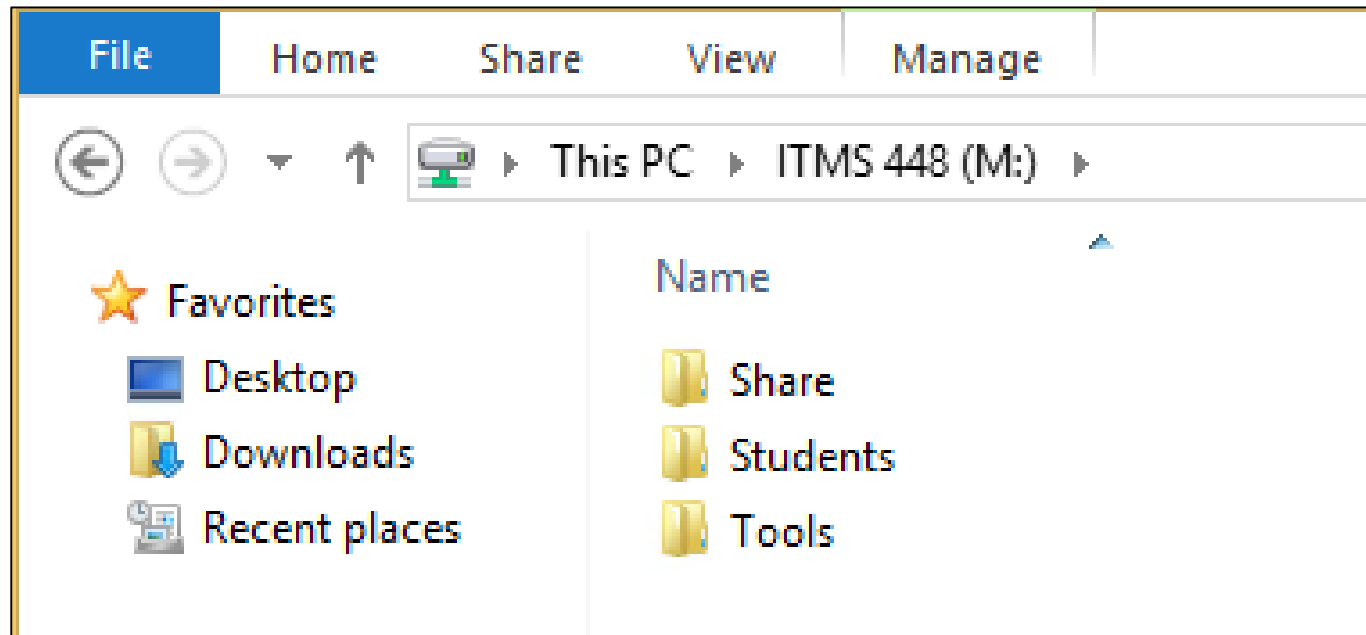
ForSec Share (M: Drive)

- ...is available from the Windows 8.1 VM



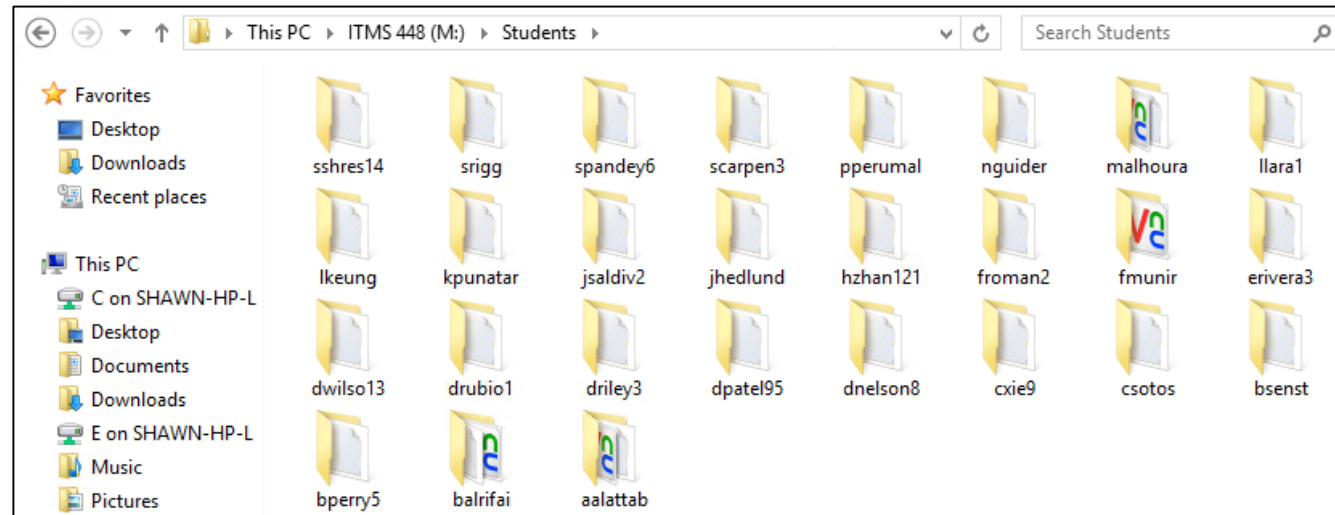
ForSec Share (M: Drive) – Shares & Tools Folders

- Shares: Holds OVA files for VirtualBox
- Tools: Holds tools you may need to install at times
 - These folders are restricted to read only



ForSec Share (M: Drive) – Students Folder

- Every Student has his/her own personal folder, which can be used to store any class related work



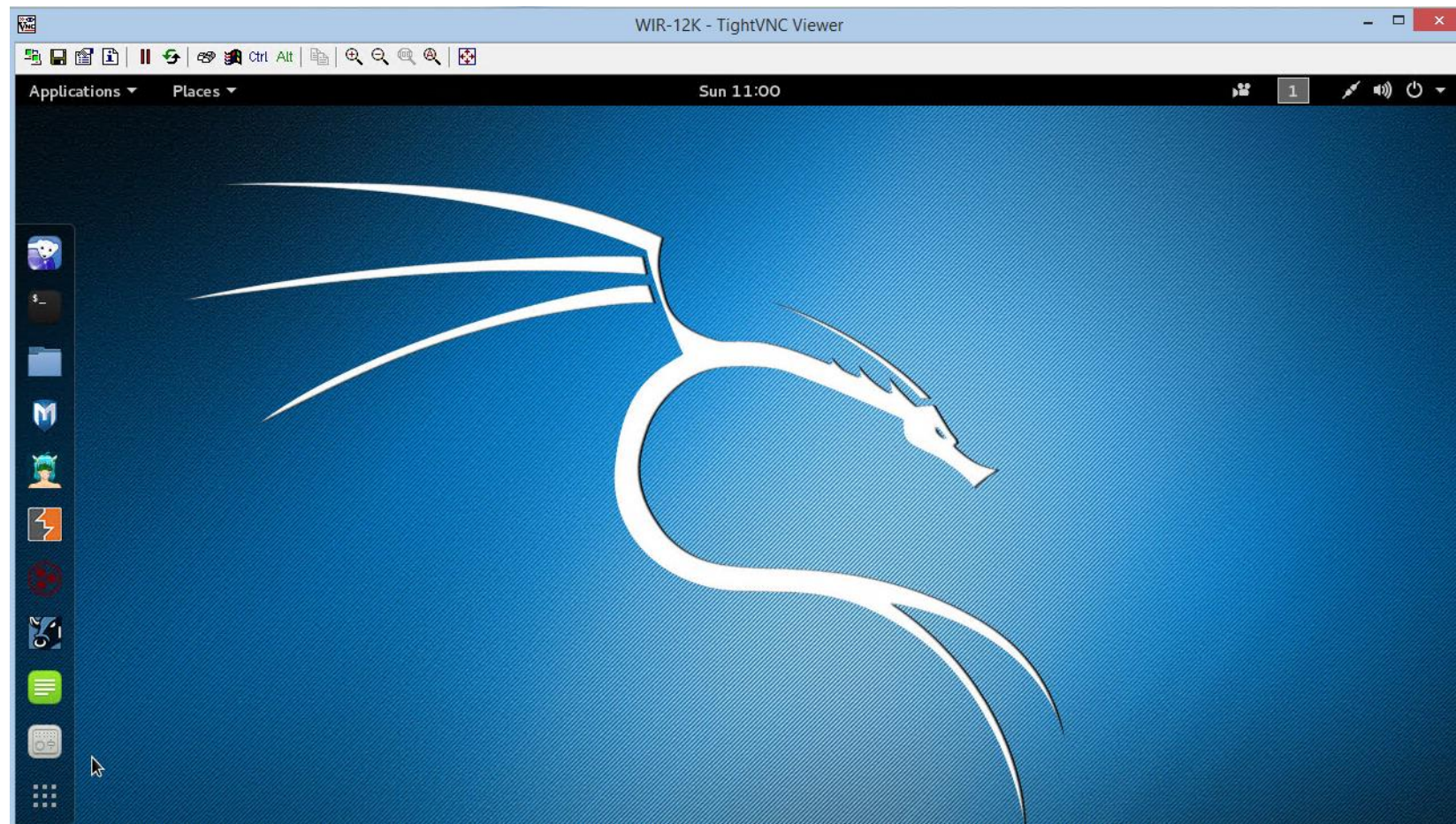
Note: Only the owner and the class instructor can access a personal folder

Kali Linux

- You will use tightVNC to access your Kali 2.0 Linux VM
- There should be a shortcut on your Win8.1 VM desktop to log you into Kali 2.0 as root
 - In general, do not update or upgrade the Kali 2.0 VM
- Additionally, there is a readme file in each of your Student folders on the (M: Drive) which contains your tightVNC credentials and IP address of your Kali VM should you need them in the future

Kali Linux Access

- Go ahead and open your Kali Linux VM

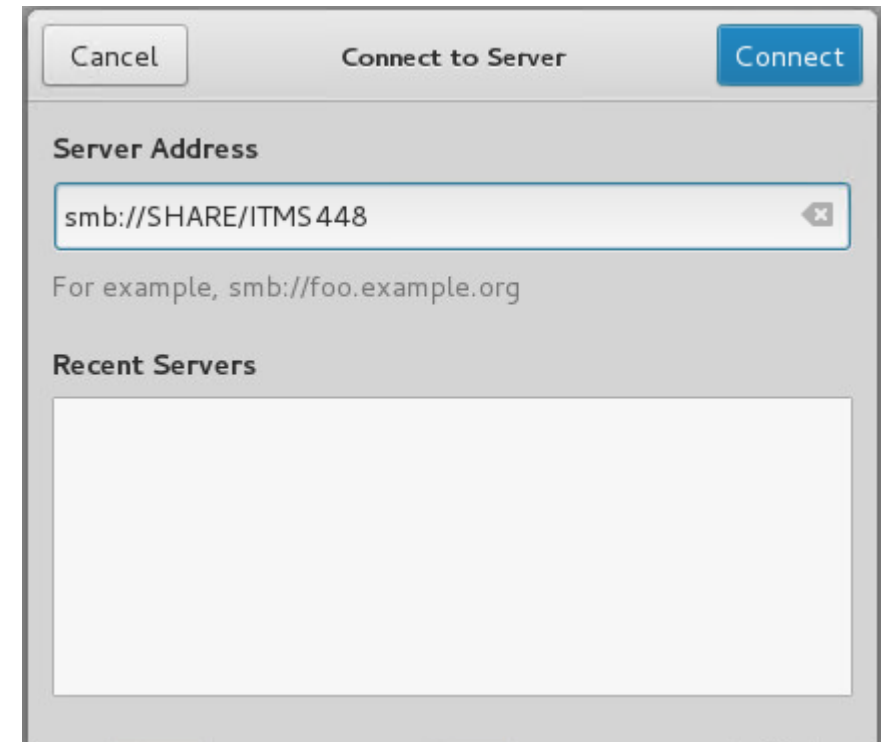


Kali VM Notes

- If you encounter the screensaver with the clock, drag it upwards to return to your logon session
- Don't ever shut down your Kali VM, just exit from VNC by clicking the Red X at the top right
- The credentials for Kali are root/toor
- Changing your display resolution will cause your VM to hang

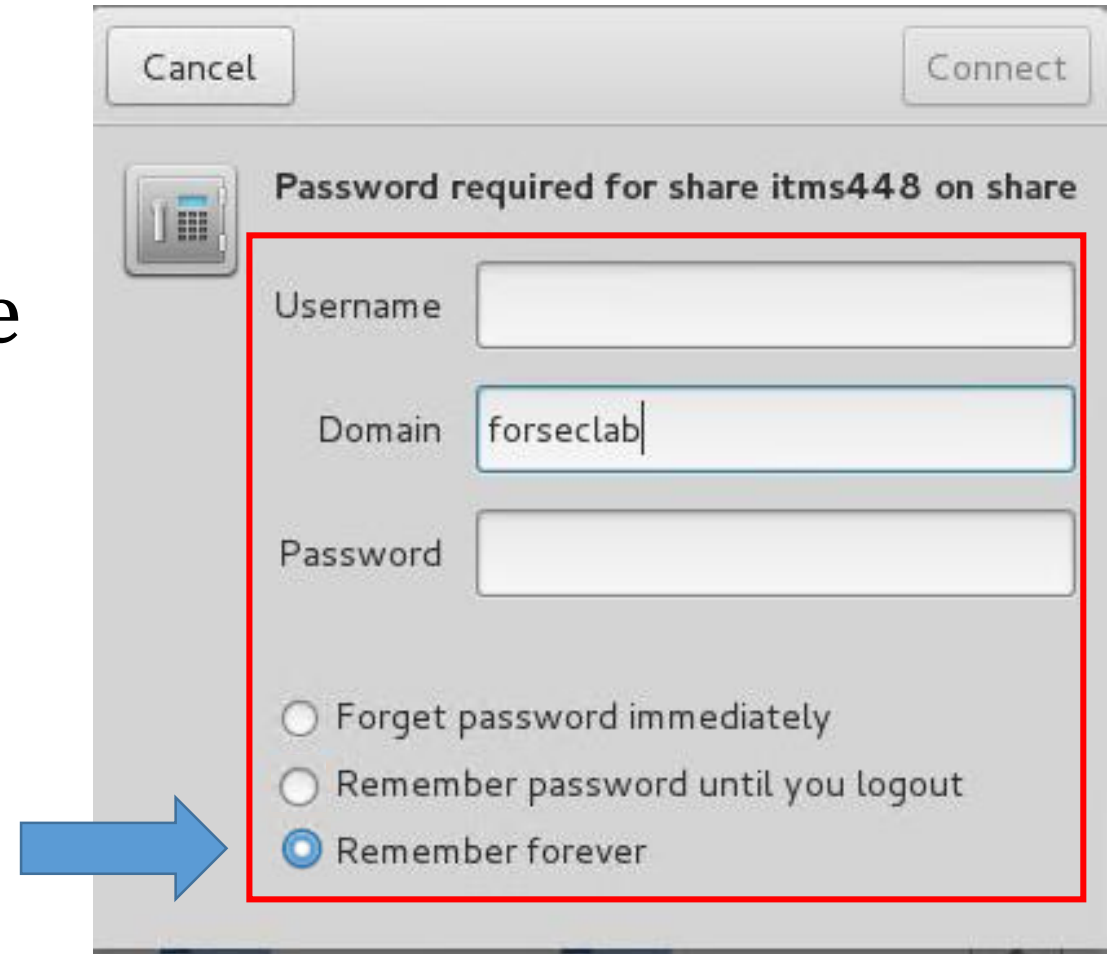
Kali Linux VM access to “M: Drive”

- Click on *Places* and then *Computer*
- Select *Connect to Server* on the bottom left
- Server Address:
 - smb://SHARE/ITMS448
 - Hit Connect



Kali Linux VM access to “M: Drive”

- In a few seconds an authentication window will appear
- Enter your RADISH username and password
- The Domain is forseclab
- Choose “Remember forever”
- Hit Connect



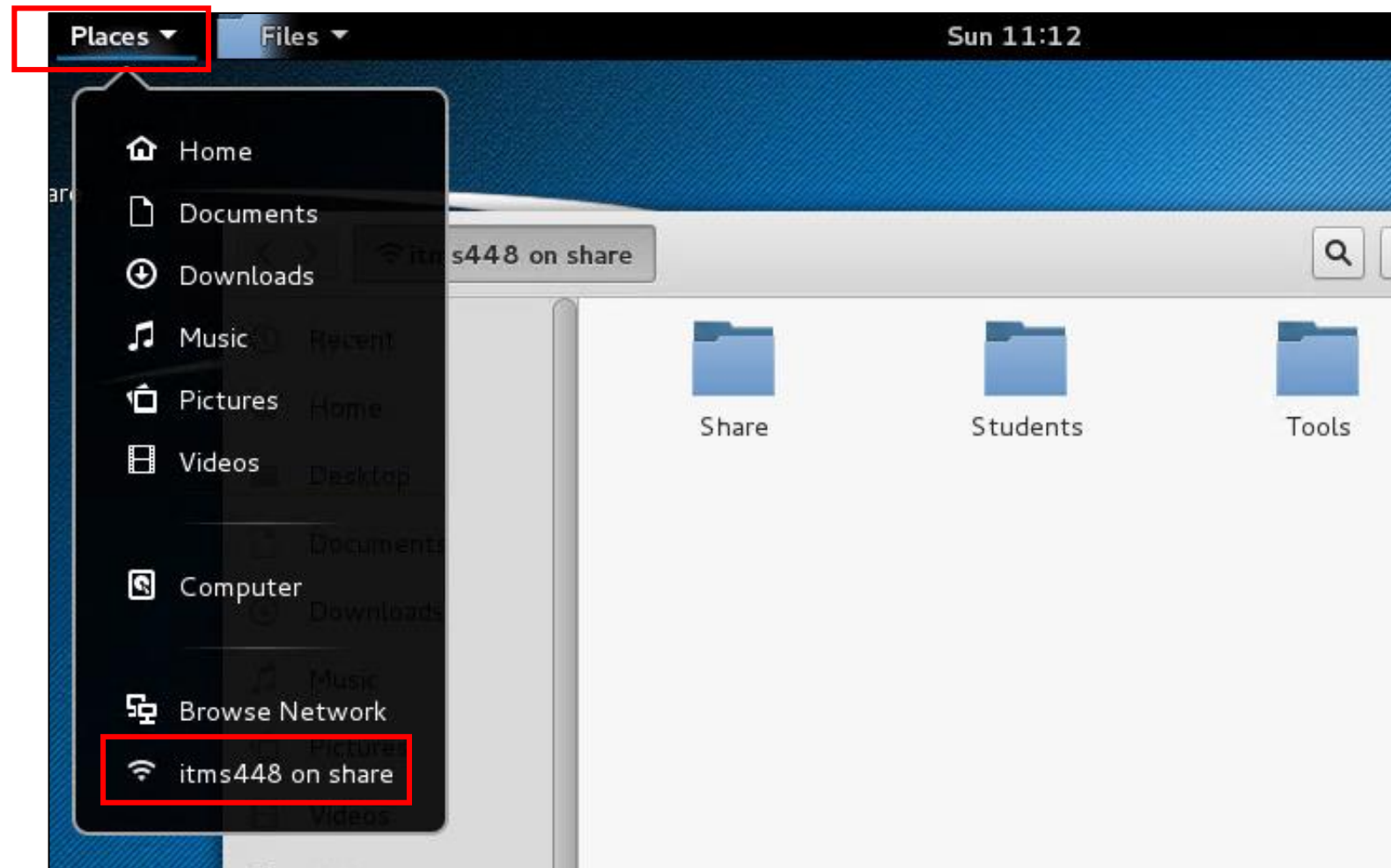
Kali Linux VM access to “M: Drive”

- Enter your Kali root user password which is:
- toor
- Hit Unlock



Kali Linux VM access to “M: Drive”

- Share will then be mounted:



Part III

Accessing Student VMs from your Personal/Home Computer via RADISH

Labs/Homework

- The Student VMs for Win 8.1 and Kali Linux will mainly be used for:
 - Homework Labs

Installation

- Dawid emailed a PowerPoint to you earlier this week along with a Google sheet. If you haven't already, after class:
 - Install the View client on your personal computer
 - Verify you can logon to your student ITMS448 VM
 - If you have any issues, email Dawid

Part V

RADISH Rules

Rules

DO NOT scan or perform any unethical activity on or using the RADISH system

It might block your access to RADISH

It will affect your class grade

Rules (Cont.)

Don't ever shut down RADISH VMs

Just close the desktop (disconnect) Click on X

Don't try to change the display resolution on your Win8.1 VM

It automatically adjusts resolution

Don't try to change the display resolution on Kali

It may hang your VM

Don't apply updates to anything at any time

Let us handle updates

If you hang your VM

Send TA or lab manager email immediately so they can restore you

Lab Manager Contact Info

- ForSec Laboratory is supported by Dawid Broda and Yalinne Castelan
- Contact them at any time if you have any questions regarding using RADISH
- They should reply to you no later than 24 hours
 - **Dawid Broda:** dbroda@iit.edu
 - **Yalinne Castelan:** ycastela@hawk.iit.edu

Questions???



Security Overview

- Slide Deck C