

Cybersecurity

Linux Scavenger Hunt

Linux 3

Let's Get Ready for a **Linux Scavenger Hunt**





Challenge

Today, you will be using a pre-configured headless Linux server and applying the skills we've learned over the past three weeks to complete a fun activity known as capture the flag (CTF).

Setting up the headless server:

Once running, you can ssh directly into the target machine



CTF Instructions and Rules



You can work alone or in teams.



If working with a team, all members must participate equally.



To complete this CTF, you will launch a headless VM and login.



You can use all previous material and internet resources.



While each member can work on different steps, most steps must be completed in order.



Professors and TAs will not be providing hints or assistance unless there are technical issues that prevent the VMs from running correctly.

Hints

1 Take note of anything interesting that you find.

2 Each flag has the following format:
`flag_1:97df27aec8c251503f5e3749eb2ddea2`

3 There are eight flags in total. The first seven flags will be combined to create the final flag.

4 Copy down any credentials you find. You may need to use them later.





Let's Get Started:

2 Hours

[CLICK TO START TIMER](#)



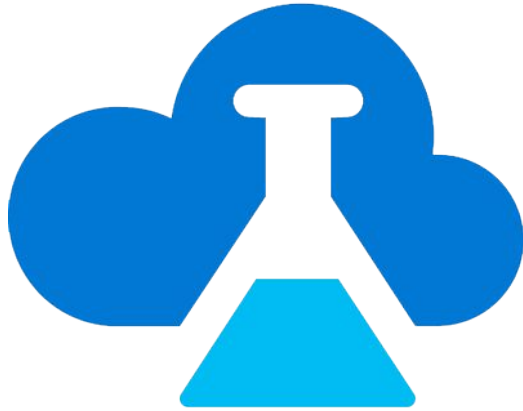
Time's up!
Let's review



Questions?



Azure Lab Set Up



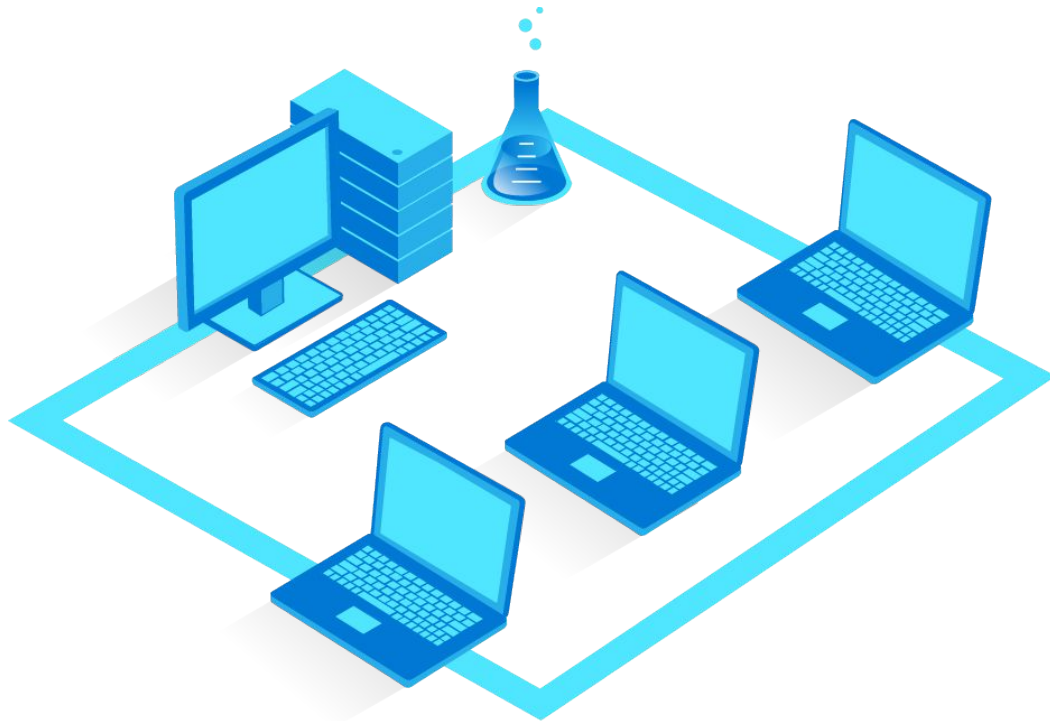
Next week, we will begin to learn system administration and security tools for one of the most popular operating systems: Windows.

For that unit, we need to use a new **Azure lab environment.**

Azure Lab Services

Up until now, we've only needed to have access to a single virtual machine.

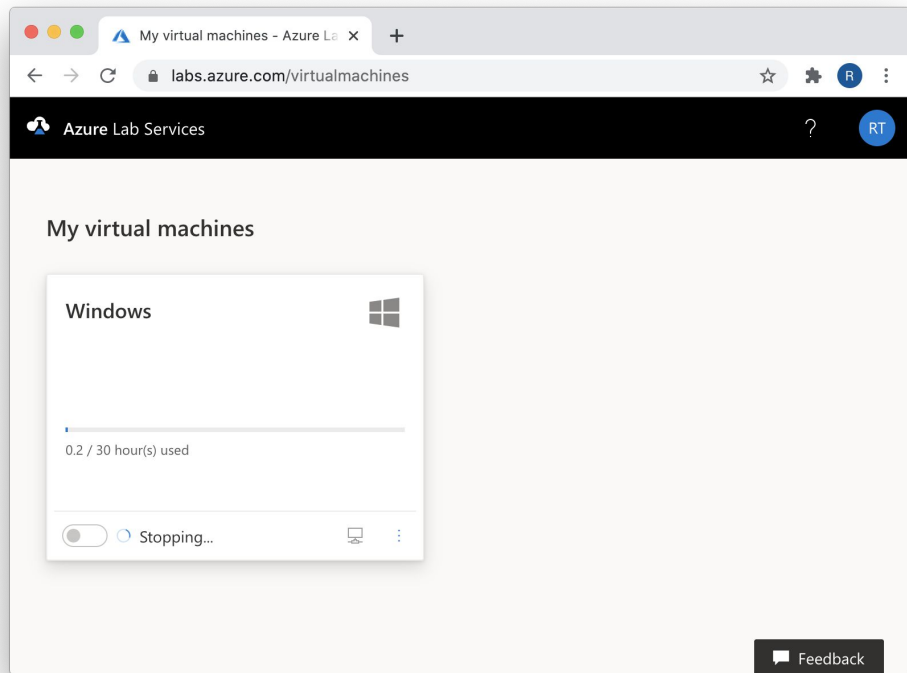
Starting next week and in several other units in the program, we will be accessing lab environments that are composed of multiple VMs.



Lab Hours Quota



Machines will start up automatically prior to class and will automatically shut down when class is over. You will have access to labs during and after class.



Outside of class hours,
each student will be provided 30 hours of
Azure lab access.

If students exceed that quota,
they will be provided an additional 10 hours.

If they exceed those additional hours,
they will be provided an additional 5 hours.
Once students exceed that final quota,
they will not be provided any additional hours.

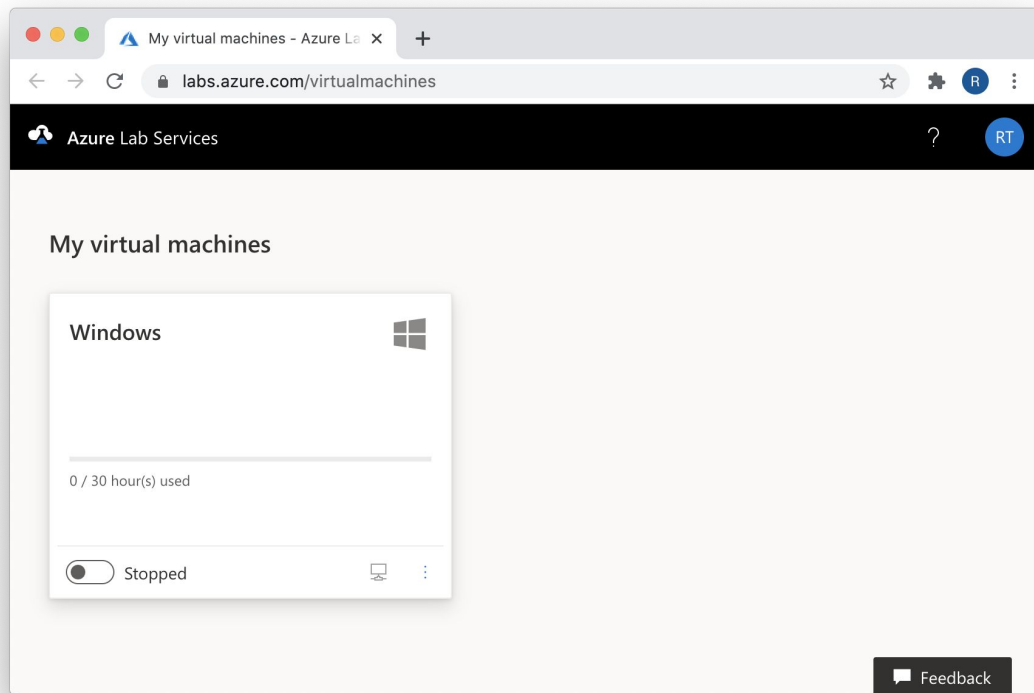
Lab Hours Quota

You must properly shut off your machines or you will lose quota hours.

It is important to properly shut off these lab environments.

If students do not, they will accidentally use up their quota hours.

Students can see how many quota hours they have remaining on the **lab environment card** in the Azure dashboard.



Retaining Lab Work

Your work will not be deleted between classes.



The machines' hard drives don't delete anything unless you choose for them to.



However, if your lab environment needs to be reset, all work will be deleted.



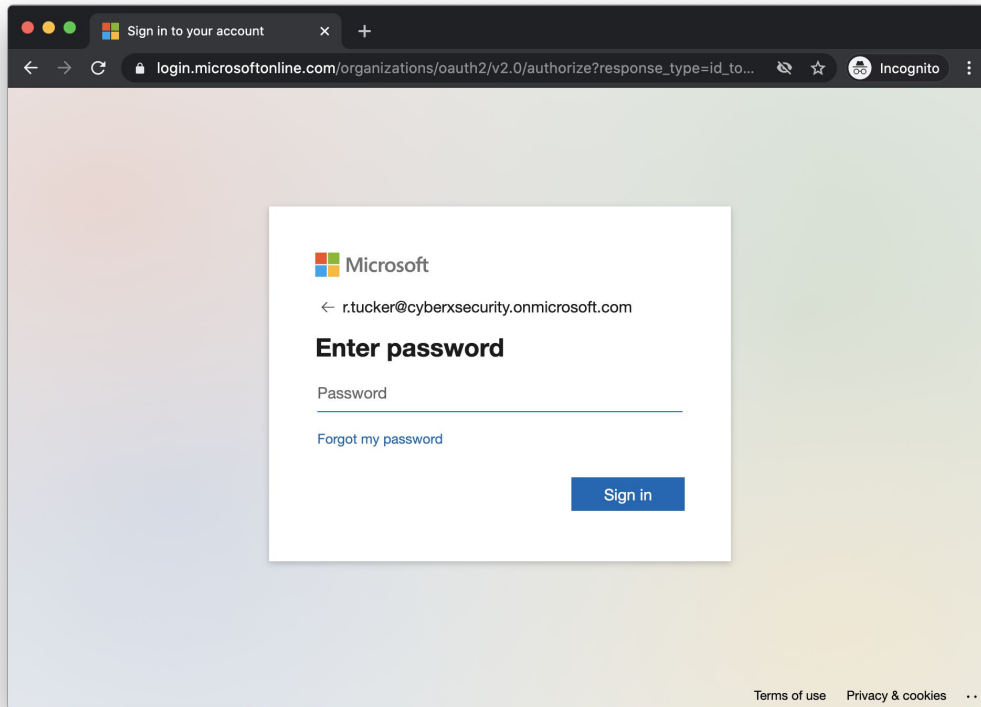
For example, VMs can be reset if you accidentally misconfigure your environment or have issues with any of the individual machines in an environment.

Remember Your Passwords!

You must remember your passwords.

When you access Azure for the first time, you will be prompted to create new passwords. It is recommended that you store these passwords using a password manager.

It will take up to **36 hours** to reset a password.





You will now receive
your **registration link**
and unique Azure
login credentials.



Logging In via RDP

We will connect to our VMs using remote desktop protocol (RDP), a proprietary protocol that allows us to log into and interact with a remote machine.

In order to use RDP, you must install an RDP Client.



macOS
RDP Client



Windows
RDP Client



Instructor **Demonstration**

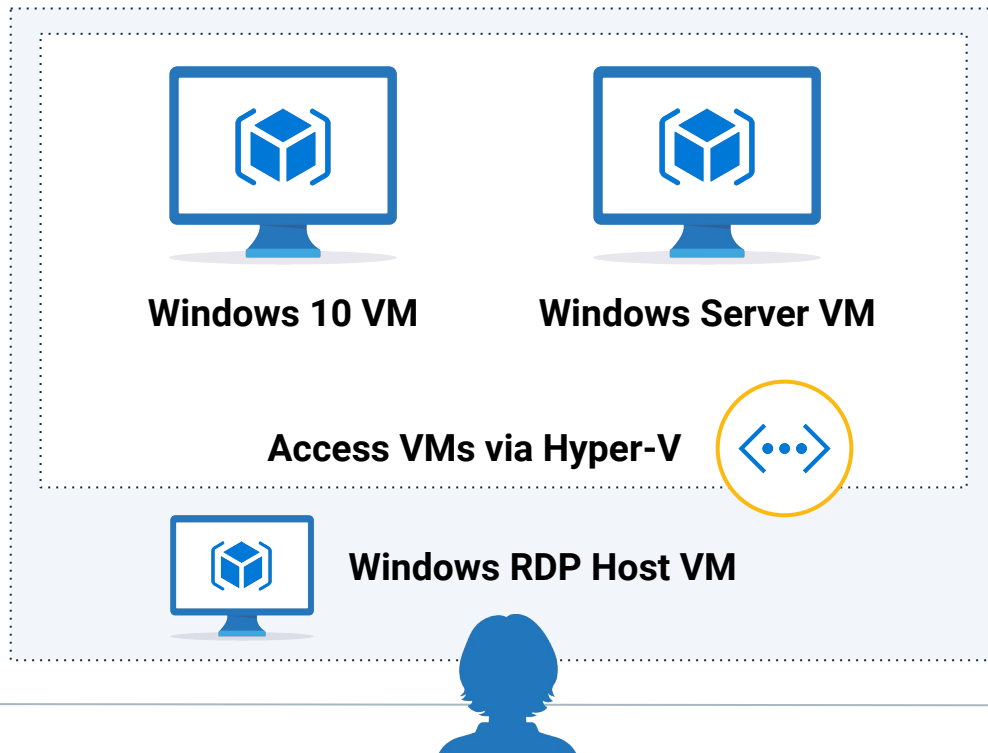
Azure RDP Demonstration

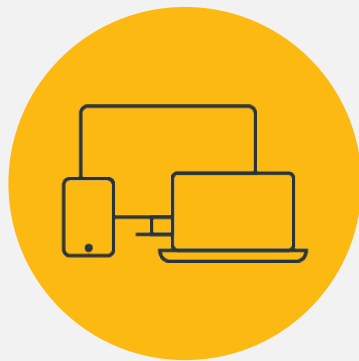
Hyper-V

All of the lab environments consist of one or more VMs running inside of a Windows host, using a technology called Hyper-V.

In other words, you will connect to a Windows computer that contains several VMs inside of it.

Therefore, even when class will use Linux operating systems or other VMs, we will still connect to a Windows machine first.





Instructor **Demonstration**

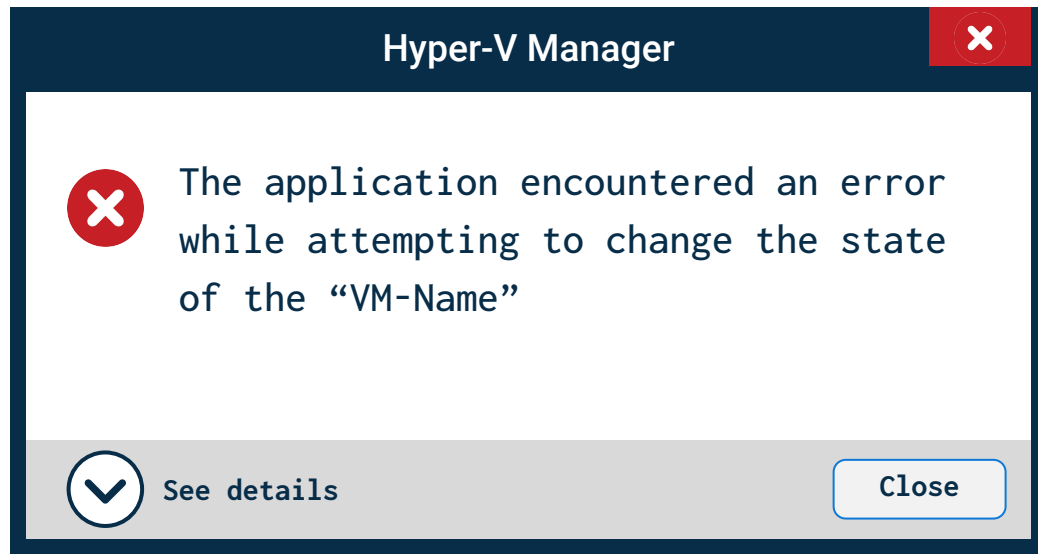
Hyper-V Manager

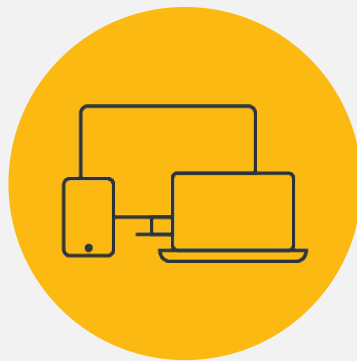
Hyper-V Saved State

Hyper-V VMs should be shut down after every session in order to avoid the Hyper-V machine going into a hibernation known as a saved state.

If a machine goes into a saved state, you may see the error: **The application encountered an error while attempting to change the state of the “VM-Name.”**

We can pre-empt this by deleting the saved state on the Hyper-V machine.





Instructor **Demonstration**

Clearing Saved State

VM Credentials

Below are the credentials for the Windows RDP Host machine.

This is the only machine you'll need for 7.1 and 7.2



Username: azadmin
Password: p4ssw0rd*

Below are the credentials for the two nested Hyper-V virtual machines. You will use these VMs on 7.3.

Credentials for the Windows 10 virtual machine



Username: sysadmin
Password: cybersecurity

Credentials for the Windows Server virtual machine

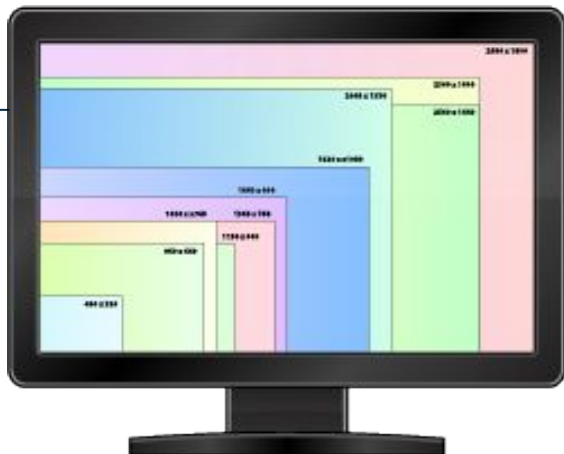


Username: sysadmin
Password: p4ssw0rd*

Adjusting Screen Resolution

Because we are using a virtualized environment for the Windows 10 machine, the screen resolution may not fill the entire screen during demos.

To adjust screen resolution:



01

Log into the **Windows 10** VM and right-click anywhere on the screen.

02

In the new tab that opened, scroll down to **Display Settings**.

03

A new Display window will pop up. Navigate to **Display resolution** and adjust the resolution to match your screen from here.



Important



You will be provided **30 hours** of Azure lab access.

- If you exceed that quota, you will be provided an additional **10 hours**.
- If they exceed those additional hours, you will be provided an additional **5 hours**.

Once you exceed that final quota, you will not be provided any additional hours.

It is extremely important that you preserve your allotted hours by **shutting off your machines** at the end of each class.

Shutting Down Your Machine

When you're done with your lab, you will need to:

Turn off the nested VMs inside of Hyper-V.

- Open the Hyper-V Manager
- Click on the Windows 10 machine in the center panel and then click Turn Off in the bottom-right pane.
- Do the same for the Windows Server VM.

Close the RDP connection to turn off the host VM.

- Simply click the red **X** in the top-left corner of the RDP window.
- This will cause the host VM to automatically turn off after 10 minutes.
- However, in order to always ensure that the environment is turned off, click the Stop button in the bottom-left of the lab card in the Dashboard.



Questions?





Break

15 mins