

# Welcome to Systems Security (SysSec)

UBNetDef, Fall 2022

Week 1

Lead Presenter: Phuong Quynh Nguyen

# Agenda - Week 1

1. Welcome
  - 1.1. Introductions
  - 1.2. Opening remarks
  - 1.3. Ground rules
  - 1.4. Learning Objectives
2. Overview
3. Virtualization
  - 3.1. In Class exercise: Login to vCenter
  - 3.2. In Class exercise: Virtualization Activity
4. Coursework
  - 4.1. Workflow
  - 4.2. Support
  - 4.3. Reporting
  - 4.4. Topology
  - 4.5. Assignment: Homework 1
    - 4.5.1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up

# Mattermost

# Introductions

## UB SecDev, Fall 2022

Phuong Quynh Nguyen (@pnnguyen) - SecDev Lead

Raymond Harenza (@rwharenz) - Internal Lockdown, Black Team

Griffin Refol (@grefol) - Lockdown Black Team, Hack the Port

Ethan Viapiano (@ethanvia) - Lockdown Black Team Shadow, CCDC, Hack the Port

# Introductions

## UB NetDef Faculty

Prof. David J. Murray (@djmmurray)

Prof. Kevin Cleary (@cleary.kevin.p)

Prof. Dominic Sellitto (@dsellitto)

## UB SecDev Alumni Volunteers

Stephen James (@stephenorjames)

Aaron Fiebelkorn (@aaron)

Nick Brase (@nickbrase)

Chris Klimek (@chrisklimek)

Shreya Lakhkar (@shreya)

Lucas Crassidis (@luke)

Phil Fox (@xphilfox)

Aibek Zhylkaidarov (@aibek)

# Opening Remarks

Featuring Prof. Murray

# UBNetDef Goals:

Learn, Have Fun, Be Your Best

# Ground Rules

- Attendance: Taken weekly during lecture time.  
IT IS PART OF YOUR GRADE!!
- Homework: Weekly, deliverables due Thursdays  
6:29 pm
- Late Policy: Late submissions are not accepted
- COVID: Follow all guidelines put forward by the  
University and SUNY



# Learning objectives

- Learn the CIA triad
- Understand the basics of virtualization
- Learn the components of the System Security class

# Agenda - Week 1

1. Welcome
  - 1.1. Introductions
  - 1.2. Opening remarks
  - 1.3. Ground rules
  - 1.4. Learning Objectives
2. Overview
3. Virtualization
  - 3.1. In Class exercise: Login to vCenter
  - 3.2. In Class exercise: Virtualization Activity
4. Coursework
  - 4.1. Workflow
  - 4.2. Support
  - 4.3. Reporting
  - 4.4. Topology
  - 4.5. Assignment: Homework 1
    - 4.5.1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up

# Overview - What is UBNetDef?

It's an organization!

We host:

- Camps
- Competitions
- Courses

As:

- Faculty
- Students (grad and undergrad)
- Alumni and volunteers

# Overview - What are UBNetDef roles?

All sorts!

- Learners
- Curriculum development
- Course instruction
- UB team competitors
- Infrastructure maintenance and management
- Mentorship and advising
- Administration (this is mostly Prof. Murray)

# Overview - UBNetDef Learners

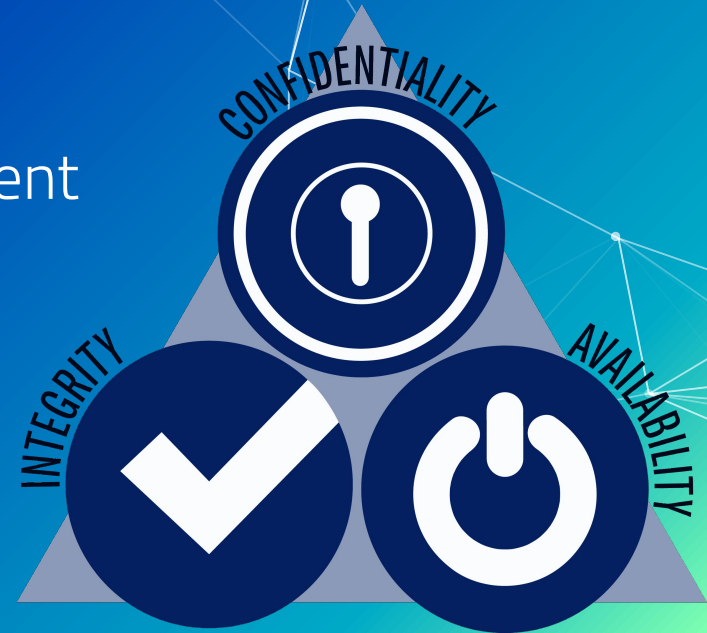
The (for-credit!) courses

- SysSec: The gateway
- Network Security (NetSec)
  - Linux software and networking deep dive
  - Packet analysis
  - Report writing
- Scripting Security
  - Bash programming
  - Security project
- Security Development (SecDev)
  - Course and curriculum development/instruction
  - **Infrastructure management**

# Overview - SysSec

What about *this* course?

- Investigating the boundaries and overlaps between:
  - Information Technology (IT)
  - Information Systems (IS) Management
  - Computer Hardware and Software
- ...through the lens of “cybersecurity”
  - Observe: The “cybersecurity triad”

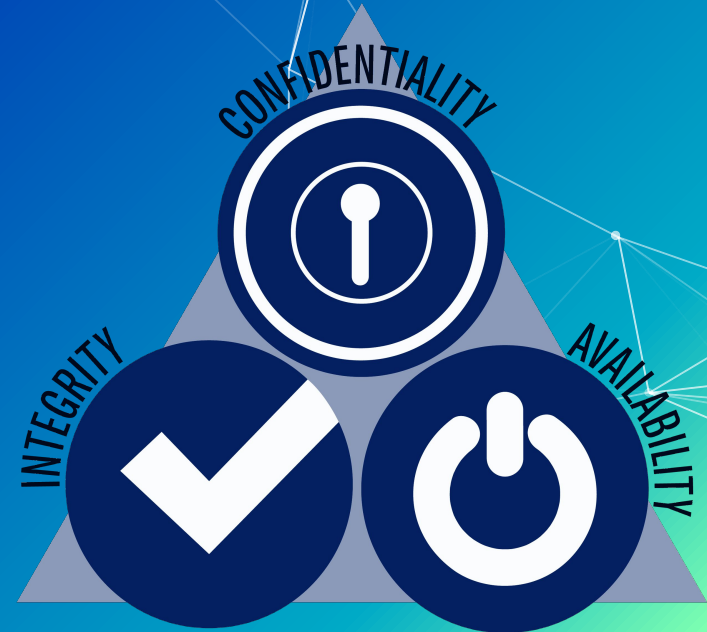




# Overview - Cybersecurity

What's the difference?

- Confidentiality
- Integrity
- Availability

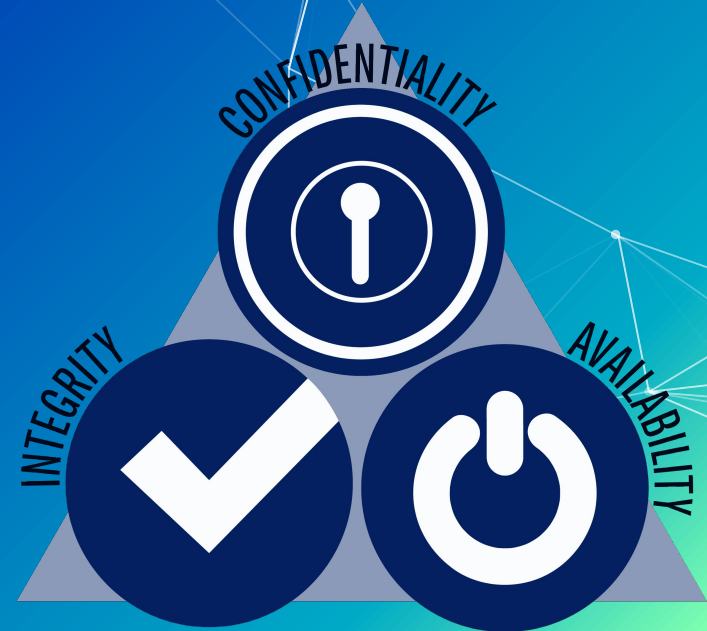


# Overview - Cybersecurity

What's the difference?

- Confidentiality
- Integrity
- Availability

Which is most important?





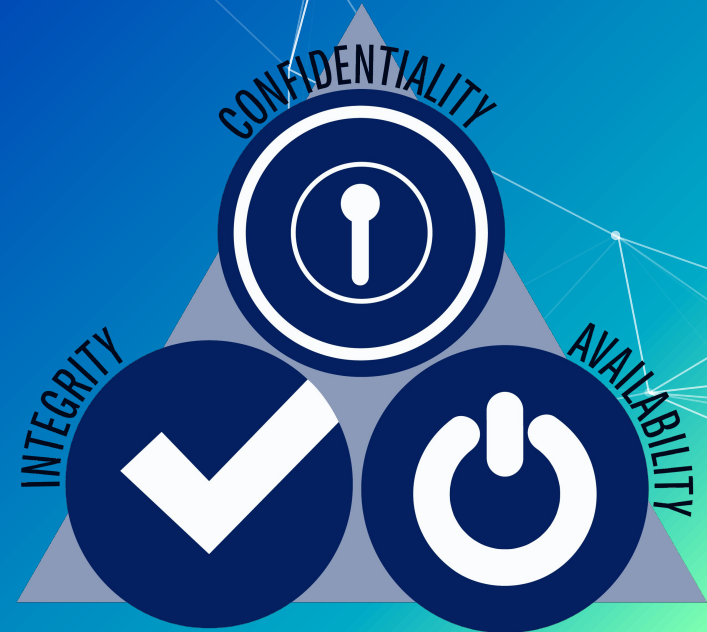
# Overview - Cybersecurity

What's the difference?

- Confidentiality
- Integrity
- Availability

Which is most important?

Can priorities between the three change?



# Overview - Cybersecurity Roles

## Discussion:

Who does what?

- Executives
- Managers
- Evaluators
  - E.g., consultants, analysts, auditors, testers
- Technicians
- Programmers/Developers
- Educators

# Overview - Cybersecurity Components

- Computer/controller software
- Network
  - Wireless
- Algorithmic/cryptographic
- Computer/controller hardware
- Physical
- Governance
- Others?

# Agenda - Week 1

1. Welcome
  - 1.1. Introductions
  - 1.2. Opening remarks
  - 1.3. Ground rules
  - 1.4. Learning Objectives
2. Overview
3. Virtualization
  - 3.1. In Class exercise: Login to vCenter
  - 3.2. In Class exercise: Virtualization Activity
4. Coursework
  - 4.1. Workflow
  - 4.2. Support
  - 4.3. Reporting
  - 4.4. Topology
  - 4.5. Assignment: Homework 1
    - 4.5.1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up

# Distribution of Class Materials

- Important Note: Please do not damage the equipment

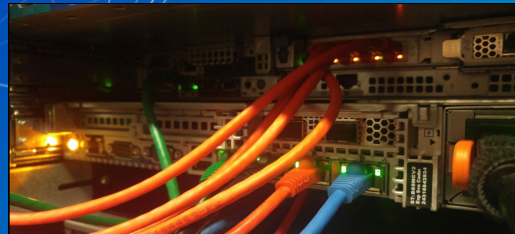
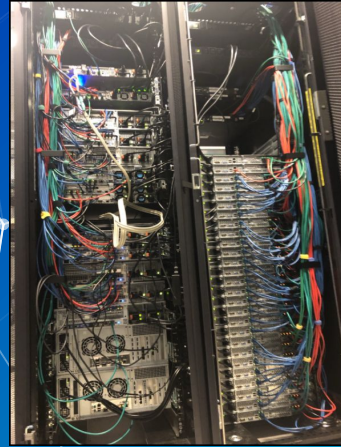


# UBNetDef Resources

As it turns out, UBNetDef has you *all* covered already. (Whew!)

**We have these:**

... and all you have to do is drive over to Davis Hall and pick your gear up.



# Converging the analog: Virtualization

Instead, we're going to get you the resources you need for this class through **virtualization**!

- Remote access to all kinds of different computing solutions
- No need for your own hardware *or software*
  - Not even a VirtualBox download (for those of you with experience)!
- Effective 24/7 access
- UB and program donors foot the bill!
  - No small expenditure

# In Class Activity

Login to vCenter



# Virtualization: Let's look inside

- ⬡ Login to VPN if off campus
- ⬡ Login to vCenter
  - ⬢ vCenter: <https://cdr-vcenter.cse.buffalo.edu/>
  - ⬢ Use your full UB email for the login ID
  - ⬢ Course links available at <https://ubnetdef.org/courses/syssec/>
    - Also available on UBLearns!
  - ⬢ Favorite/Bookmark vCenter!



# **In Class Activity**

Virtualization Activity

# Virtualization Activity

- Windows
  - Open your Windows1
    - User: `sysadmin`
    - Password: `Change.me!`
  - Try to use it. What do you observe?

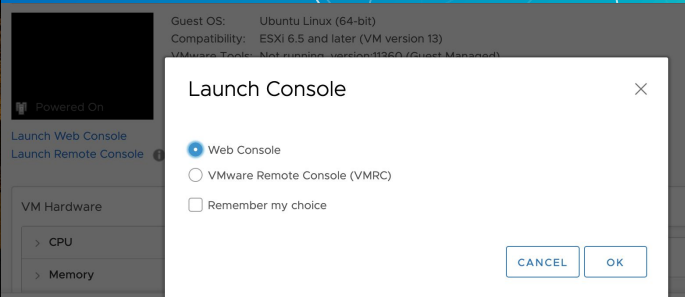
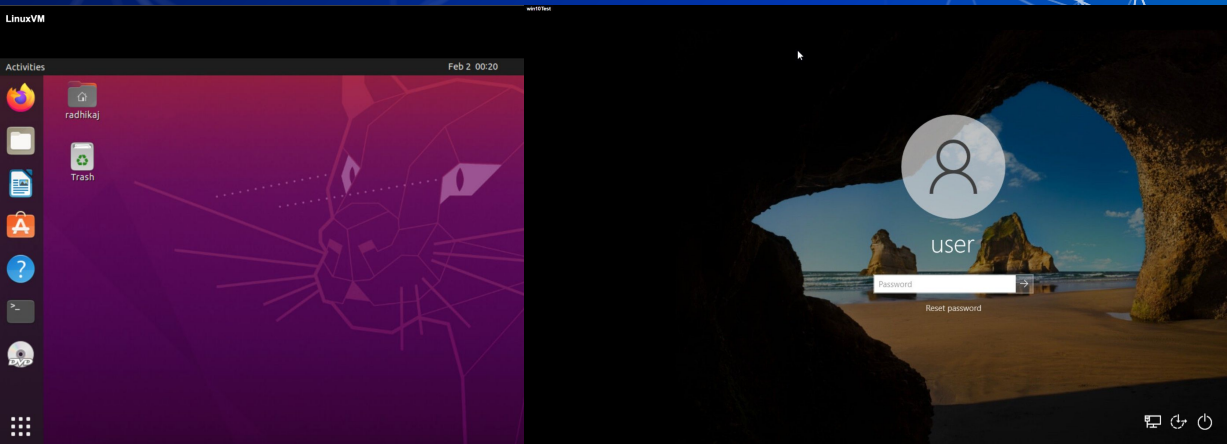
# Virtualization Activity

- Windows
  - Open your Windows1
  - Try to use it. What do you observe?
  - And now, open Windows2
    - User: `sysadmin`
    - Password: `Change.me!`
  - What do you observe?

# Back to virtualization: How did we do that?

- A **virtual machine** is a computer inside a computer.
- A **hypervisor** lets you interact with **virtualized machines**!
- VMWare's vSphere presents the **hypervisor** to you!

Launch Web Console  
Launch Remote Console



# **Break slide**

Please return on time!

# Agenda - Week 1

1. Welcome
  - 1.1. Introductions
  - 1.2. Opening remarks
  - 1.3. Ground rules
  - 1.4. Learning Objectives
2. Overview
3. Virtualization
  - 3.1. In Class exercise: Login to vCenter
  - 3.2. In Class exercise: Virtualization Activity
4. Coursework
  - 4.1. Workflow
  - 4.2. Support
  - 4.3. Reporting
  - 4.4. Topology
  - 4.5. Assignment: Homework 1
    - 4.5.1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up



# SysSec Coursework

- Assigned weekly
- Delivery and turn-in via UBLearns
  - Required .pdf format uploads
- Select weeks: System state
  - Scored separate of report deliverable
  - Full credit system state may be required for in class activities
- Due the subsequent **Thursday, 6:29 pm**



# Coursework Support

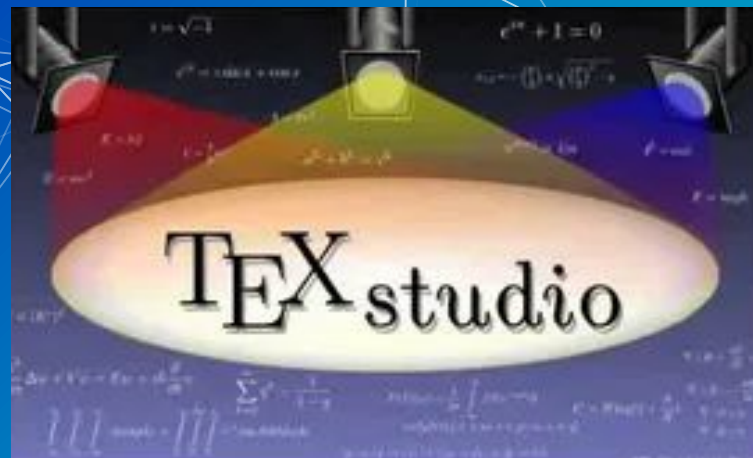
- Office hours (as posted on the <https://ubnetdef.org/courses/syssec> course page)
- General support in the Systems Security Mattermost channel
  - Subject to availability
  - Limited availability on Thursdays before class
- Open Source Research
- Peer collaboration to achieve system state is acceptable

# Weekly coursework components

- Instructional Reports
  - Screenshot technical walk-through
- Informational Reports
  - Written professional report
- Topology
  - Visual network diagram
- A style guide will be released for each component

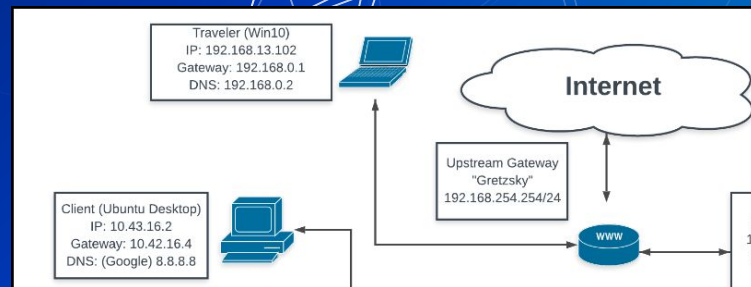
# Homework: LaTeX

- Markup language which makes formatting consistent and easy.
- Applicable to any field and future classes.
- TexStudio for Windows, Overleaf for MacOS, Linux has everything.

The Overleaf logo is displayed on a green rectangular background. It features a white stylized leaf icon to the left of the word "Overleaf" in a white, sans-serif font.

# Common coursework component: Topology

- Topology: A network diagram
- Requirements
  - Generated with a diagram platform
    - [draw.io](https://draw.io)/[diagrams.net](https://diagrams.net) (recommended)
    - Lucidchart
    - Others that look as or more professional
  - Professional organization of network
  - All devices represented as if physically available
  - Device details correspond exactly to system states



# Common coursework component: System State Remedy

- Some assignments are dependent on the completion of others.
  - Deliverables will specify a requisite, gradable “system state.”
  - This state can be a “prerequisite” for the next assignment
- We will provide near-term feedback for remediation.
- Address remediation instructions seriously!
  - If not remediated, you may not be able to participate in class or start the next HW!
  - Seek after-class help.



# Homework 1 (HW01)

- Posted to UBLearns by 9:30 pm
- Install two clients from .iso on your network segment/vCenter folder
  - Client 1: Windows 10
  - Client 2: Ubuntu Linux Desktop version 22.04 (Jammy Jellyfish)
  - All usernames and passwords must match:
    - sysadmin
    - Change.me!
- Perform simple network tests on each using the CLI. Take screenshots!
- System state: Both client installations are complete and are network-connected.
- Provide a topology of your network

# In Class Activity

Launch a new VM from ISO

# Launch a VM from a new .iso

- ⬡ In vCenter:
  - ⬡ Right click on the VM referenced in the HW
  - ⬡ Click on Edit Settings...
  - ⬡ Scroll down to CD/DVD drive 1
  - ⬡ From the drop down select Datastore ISO File
  - ⬡ Select cdr-iscsi1
  - ⬡ Scroll down to ISOs
  - ⬡ Select either a Windows or Linux ISO. Consult HW for the name.
  - ⬡ Click OK and make sure the connected option is checked



# Agenda - Week 1

1. Welcome
  - 1.1. Introductions
  - 1.2. Opening remarks
  - 1.3. Ground rules
  - 1.4. Learning Objectives
2. Overview
3. Virtualization
  - 3.1. In Class exercise: Login to vCenter
  - 3.2. In Class exercise: Virtualization Activity
4. Coursework
  - 4.1. Workflow
  - 4.2. Support
  - 4.3. Reporting
  - 4.4. Topology
  - 4.5. Assignment: Homework 1
    - 4.5.1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up

# Summary and wrap-up

Today's achievements:

- We met each other
- We learned about what UBNetDef is
- We talked about the **cybersecurity triad** at a **high** level
- We did some **virtualization**
  - Launch a machine
  - Experienced the difference between hardware settings
- We communicated the standards for **reporting**
- We described the homework process, this week's HW, and course resources

# Parting questions

Now is the time!

# **Class dismissed**

See you next week!