

Welcome to Systems Security (SysSec)

UBNetDef, Spring 2023

Week 1

Lead Presenter: Phuong Quynh Nguyen

Agenda - Week 1

1. Welcome
 1. Introductions
 2. Opening remarks
 3. Ground rules
 4. Learning Objectives
2. Overview
3. Virtualization
 1. In Class exercise: Login to vCenter
 2. In Class exercise: Virtualization Activity
4. Coursework
 1. Workflow
 2. Support
 3. Reporting
 4. Topology
 5. Assignment: Homework 1
 1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up

Mattermost

Introductions

UB SecDev, Spring 2023

Phuong Quynh Nguyen (**@pnnguyen**) - SecDev Lead

Raymond Harenza (**@rwharenz**) - Black Team

Ethan Viapiano (**@ethanvia**) - Black Team Lead

Brennan Salvadori (**@brennan5**) - Black Team

Dikshit Khandelwal (**@dikshitkhandelwal**) - Black Team

Introductions

UB NetDef Faculty

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

Prof. Dominic Sellitto (@dsellitto)

Prof. David J. Murray (@djmurray)

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. Cleary

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. Introductions
 2. Opening remarks
 3. Ground rules
 4. Learning Objectives
2. Overview
3. Virtualization
 1. In Class exercise: Login to vCenter
 2. In Class exercise: Virtualization Activity
4. Coursework
 1. Workflow
 2. Support
 3. Reporting
 4. Topology
 5. Assignment: Homework 1
 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. Cleary)

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



Think like an Adversary

How do you do it?

- Playing hide and seek.
- Hiding something valuable.
- "Robbing a bank, where do you look for money" - Vasu



Defense in Depth

What does it mean?

- Multiple layers of protection
- Backup plans
- One extra is none extra



Overview - Cybersecurity

What's the difference?

- Confidentiality
- Integrity
- Availability

Which is most important?

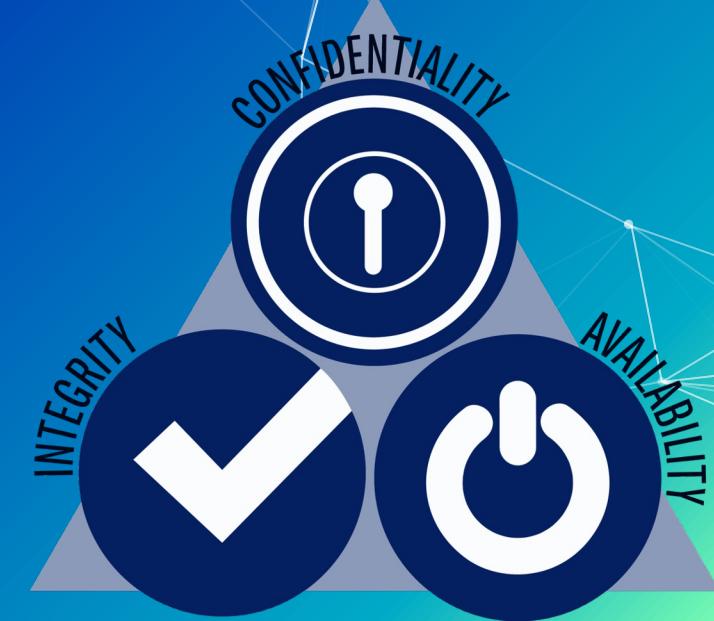


Overview - Cybersecurity

What's the difference?

- Confidentiality
- Integrity
- Availability

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. Introductions
 2. Opening remarks
 3. Ground rules
 4. Learning Objectives
2. Overview
3. Virtualization
 1. In Class exercise: Login to vCenter
 2. In Class exercise: Virtualization Activity
4. Coursework
 1. Workflow
 2. Support
 3. Reporting
 4. Topology
 5. Assignment: Homework 1
 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 YourUBITName@vsphere.local for the login ID
 - ◊ You will be sent a message with your login information
 - ◊ Course links available at <https://ubnetdef.org/courses/syssec/>
Also available on UBLearn!
 - ◊ Favorite/Bookmark vCenter!

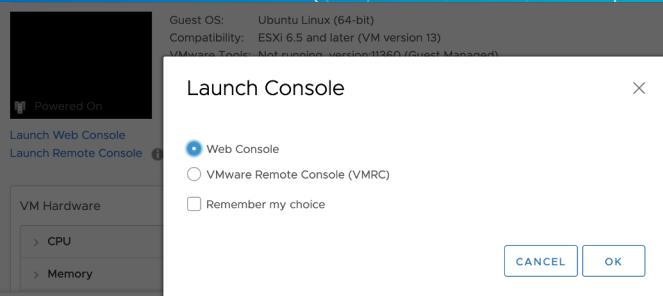
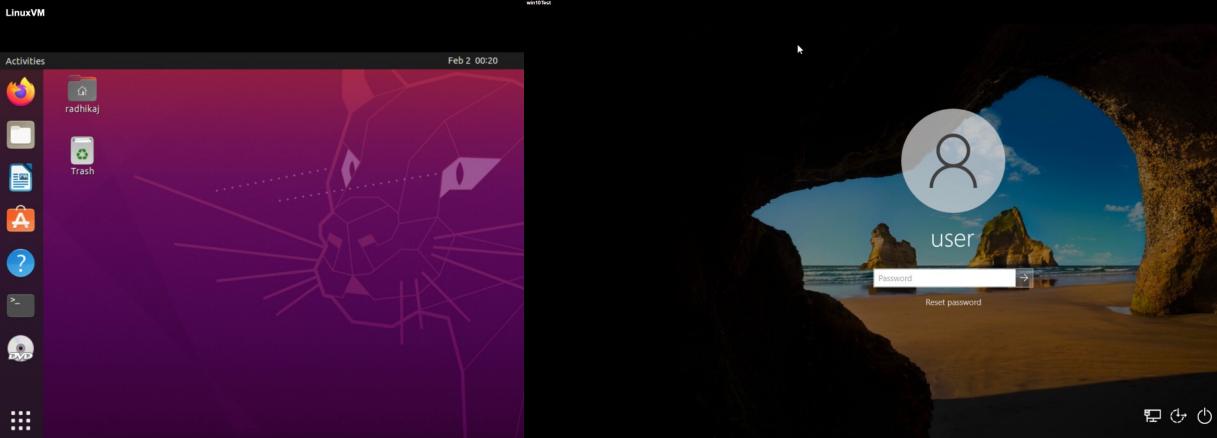
In Class Activity

Virtualization Activity

Back to virtualization: How did we do that?

[Launch Web Console](#)
[Launch Remote Console](#)

- 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!



Break slide

Please return on time!

Agenda - Week 1

1. Welcome
 1. Introductions
 2. Opening remarks
 3. Ground rules
 4. Learning Objectives
2. Overview
3. Virtualization
 1. In Class exercise: Login to vCenter
 2. In Class exercise: Virtualization Activity
4. Coursework
 1. Workflow
 2. Support
 3. Reporting
 4. Topology
 5. Assignment: Homework 1
 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 UBLearn
 - 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

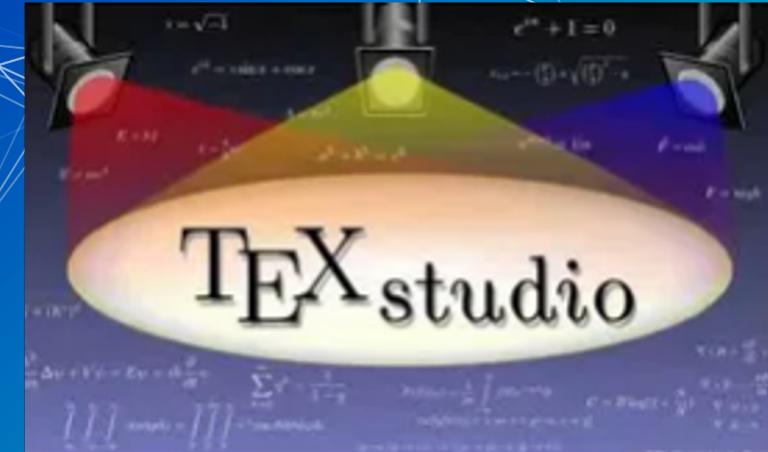
- Office hours (as posted on the
<https://ubnetdef.org/courses/syssec> course page)
- General support in the Systems Security Mattermost channel
 - Subject to availability
 - Limited availability on Thursdays before class
- Open Source Research
- Peer collaboration to achieve system state is acceptable

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

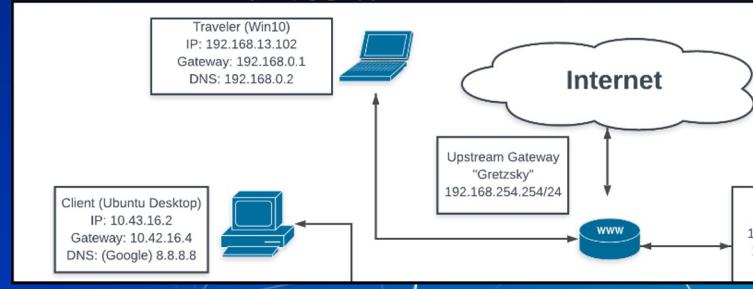
Homework: LaTeX

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



Common coursework component: Topology

- Topology: A network diagram
- Requirements
 - Generated with a diagram platform
 - draw.io/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 UBLearn 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 22.10 (Kinetic Kudu)
 - 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

- ⑥ 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. Introductions
 2. Opening remarks
 3. Ground rules
 4. Learning Objectives
2. Overview
3. Virtualization
 1. In Class exercise: Login to vCenter
 2. In Class exercise: Virtualization Activity
4. Coursework
 1. Workflow
 2. Support
 3. Reporting
 4. Topology
 5. Assignment: Homework 1
 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!