Welcome to Systems Security (SysSec)

UBNetDef, Fall 2023
Week 1
Lead Presenter(s): SecDev

Opening Remarks

Featuring Prof. Cleary

Agenda – Week 1

- Welcome
  - Introduction
  - What is UBNetDef
- Class Overview
  - Learning outcomes
  - Course requirements
- CIATD
- Virtualization
  - In class exercise: Login to vCenter
  - In class exercise: Virtualization Activity
- Coursework
  - Workflow
  - Reporting
  - Topology
  - Assignment: Homework 1
    - In class exercise: Launch a new virtual machine (VM) from .iso
- Summary/Wrap-up

Introductions

UB SecDev, Spring 2023

Raymond Harenza (**@rwharenz**) - SecDev Lead, Black Team

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

Dikshit Khandelwal **(@dikshitkhandelwal)** -

Lauren Moore **(@lbmoore)** - Black Team

Steffi Yeh **(@cyeh4)** -

Austin Chen **(@aechen2)** - Black Team

Jonathan Pestinger **(@jlpestin)** -

Kyle Lemma **(@kylelemm)** -

Overview - What is UBNetDef?

It’s an organization!

We host:

- Camps
- Competitions
- Courses

As:

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

Introductions

UB NetDef Faculty

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

Prof. Dominic Sellitto (@dsellitto)

Prof. David J. Murray (@djmurray)

UB NetDef Student Volunteers

Griffin Refol **(@grefol)**

Vasu Baldwa **(@vasudevb)** - Red Team Lead

Blake Turner **(@blaketnr)**

Radhika Jois **(@radhikaj)**

UB SecDev Alumni Volunteers

Phil Fox (@xphilfox)

Anthony Magrene (@magrene)

Bradley Manley (@smanly)

Stephen James (@stephenorjames)

Chris Klimek (@chrisklimek)

Shreya Lakhkar (@shreya)

Lucas Crassidis (@luke)

Aibek Zhylkaidarov (@aibek)

UBNetDef Goals:

Learn, Have Fun, Be Your Best

Mattermost

- Go to:
  - https://chat.ubnetdef.org/signup_user_complete/?id=j3zqpf4qubb1uppc3a1fob61wr
- Use your UB Email to sign up and use your UBIT ID as your username
- Once logged in look under public channels and press "More..." to join the channel SysSec Fall 2023

Agenda – Week 1

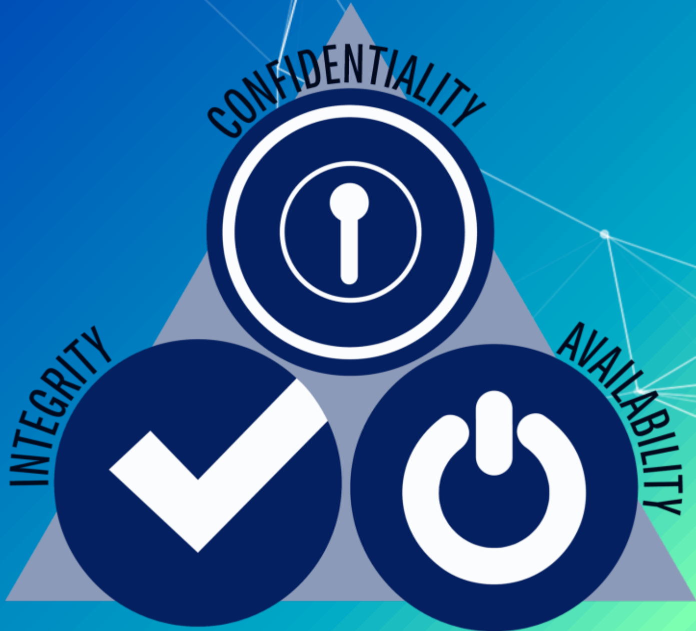
- Welcome
  - Introduction
  - What is UBNetDef
- Class Overview
  - Learning outcomes
  - Course requirements
- CIATD
- Virtualization
  - In class exercise: Login to vCenter
  - In class exercise: Virtualization Activity
- Coursework
  - Workflow
  - Reporting
  - Topology
  - Assignment: Homework 1
    - In class exercise: Launch a new virtual machine (VM) from .iso
- Summary/Wrap-up

Learning Outcomes of This Class

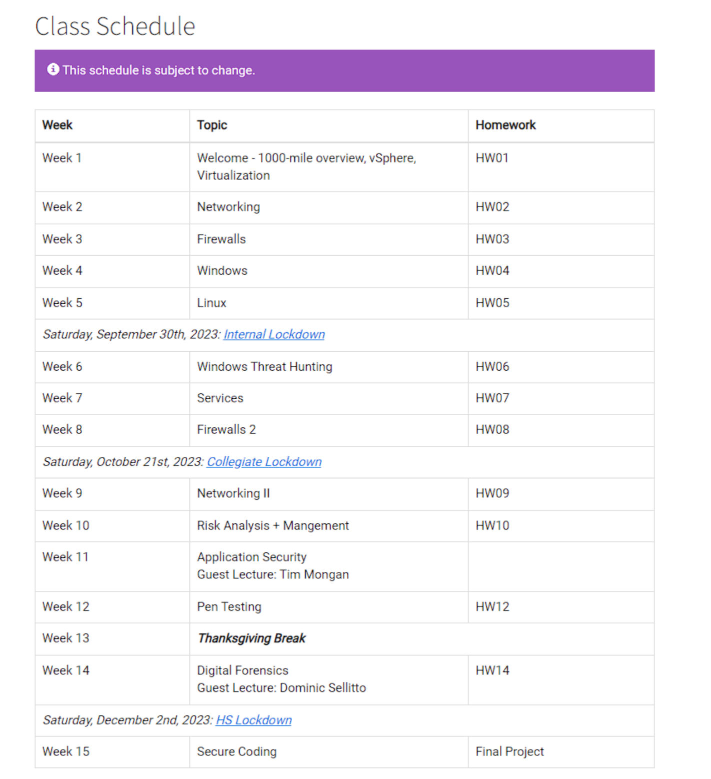
- Learn and apply basic security concepts
- Identify threats and vulnerabilities of systems
- Learn to harden systems and address vulnerabilities
  - Specific focus on Windows and Linux
- Effectively communicate via written reports
  - Documentation (instructional reports)
  - Executive and technical communication (informational reports)
- Work effectively as a team

Overview - SysSec

- 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"



Tentative Class Schedule

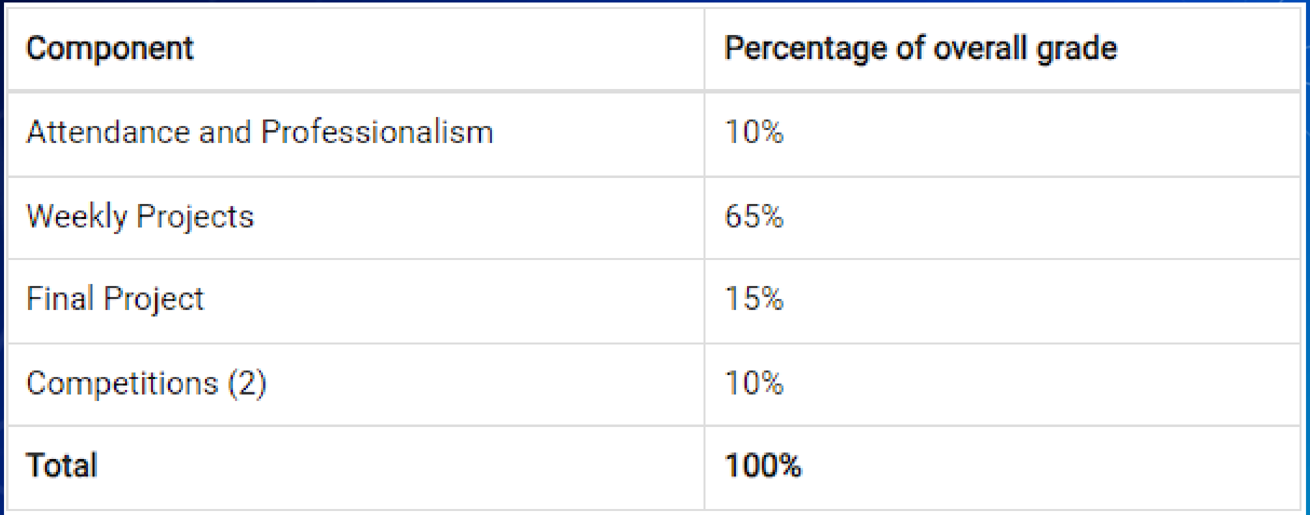


Class Schedule

ℹ This schedule is subject to change.

Week	Topic	Homework
Week 1	Welcome - 1000-mile overview, vSphere, Virtualization	HW01
Week 2	Networking	HW02
Week 3	Firewalls	HW03
Week 4	Windows	HW04
Week 5	Linux	HW05
Saturday, September 30th, 2023: *Internal Lockdown*		
Week 6	Windows Threat Hunting	HW06
Week 7	Services	HW07
Week 8	Firewalls 2	HW08
Saturday, October 21st, 2023: *Collegiate Lockdown*		
Week 9	Networking II	HW09
Week 10	Risk Analysis + Mangement	HW10
Week 11	Application Security Guest Lecture: Tim Mongan	
Week 12	Pen Testing	HW12
Week 13	***Thanksgiving Break***	
Week 14	Digital Forensics Guest Lecture: Dominic Sellitto	HW14
Saturday, December 2nd, 2023: *HS Lockdown*		
Week 15	Secure Coding	Final Project

Course Requirements



Component	Percentage of overall grade
Attendance and Professionalism	10%
Weekly Projects	65%
Final Project	15%
Competitions (2)	10%
Total	**100%**

Ground Rules

- Attendance: Taken weekly during lecture time
- Homework: Weekly, deliverables due Thursdays 6:29 pm
- Late Policy: Late submissions are not accepted

Competitions!

- UB Internal Lockdown
    - September 30th!
    - Sign up form: https://forms.gle/k8eURawkyL1vcNJG9
- External Competitions

Agenda – Week 1

- Welcome
  - Introduction
  - What is UBNetDef
- Class Overview
  - Learning outcomes
  - Course requirements
- CIATD
- Virtualization
  - In class exercise: Login to vCenter
  - In class exercise: Virtualization Activity
- Coursework
  - Workflow
  - Reporting
  - Topology
  - Assignment: Homework 1
    - In class exercise: Launch a new virtual machine (VM) from .iso
- Summary/Wrap-up

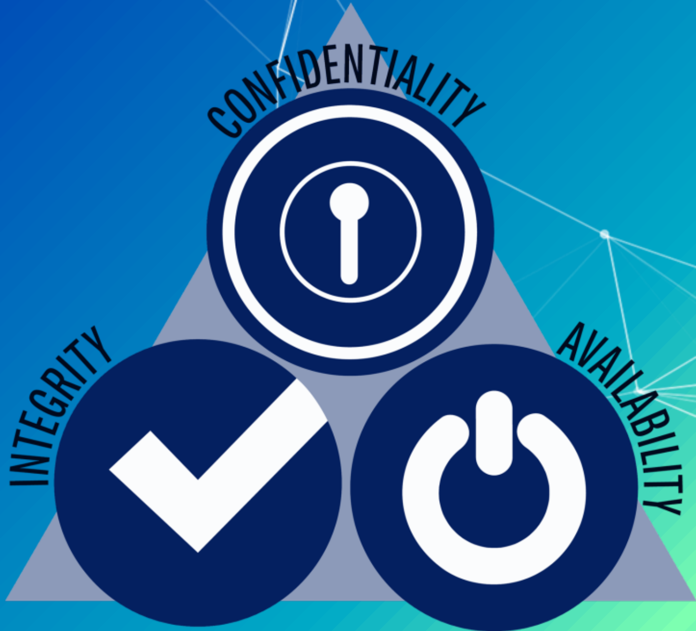
Learning objectives

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

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?

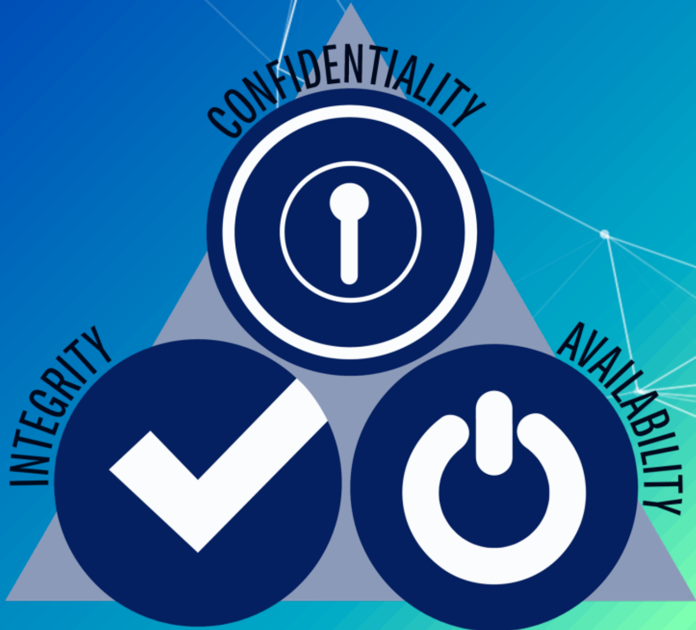
- Multiple layers of protection
- Backup plans
- One extra is none extra

Overview - Cybersecurity

What's the difference?

- Confidentiality
- Integrity
- Availability

Which is most important?

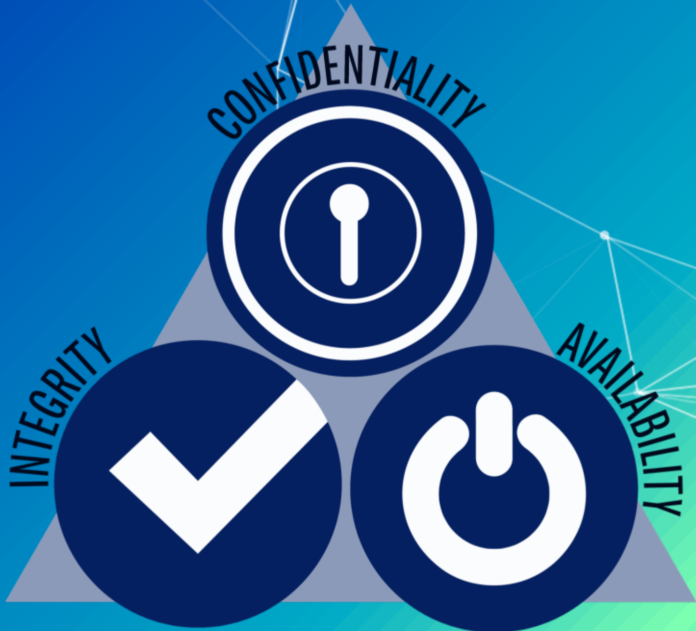


Overview - Cybersecurity

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
- Cybersecurity Engineers
- Programmers/Developers
- Educators
- End users
- Others...

Agenda – Week 1

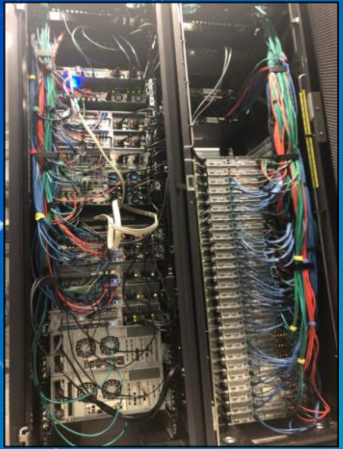
- Welcome
  - Introduction
  - What is UBNetDef
- Class Overview
  - Learning outcomes
  - Course requirements
- CIATD
- Virtualization
  - In class exercise: Login to vCenter
  - In class exercise: Virtualization Activity
- Coursework
  - Workflow
  - Reporting
  - Topology
  - Assignment: Homework 1
    - In class exercise: Launch a new virtual machine (VM) from .iso
- Summary/Wrap-up

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
- UB and program donors foot the bill!
  - No small expenditure

In Class Activity

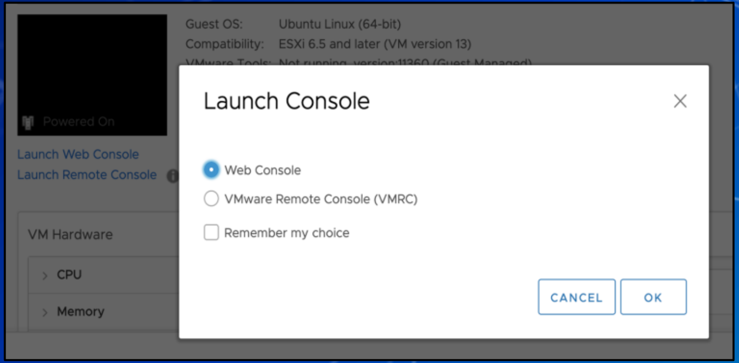
Login to vCenter

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 UBLearns!
  - Favorite/Bookmark vCenter!

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!



Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 6.5 and later (VM version 13)
VMware Tools: Not running, version:11360 (Guest Managed)

Powered On

Launch Web Console
Launch Remote Console

VM Hardware
- CPU
- Memory

Launch Console

● Web Console
○ VMware Remote Console (VMRC)
□ Remember my choice

Break slide

Please return on time!

Agenda – Week 1

- Welcome
  - Introduction
  - What is UBNetDef
- Class Overview
  - Learning outcomes
  - Course requirements
- CIATD
- Virtualization
  - In class exercise: Login to vCenter
  - In class exercise: Virtualization Activity
- Coursework
  - Workflow
  - Reporting
  - Topology
  - Assignment: Homework 1
    - In class exercise: Launch a new virtual machine (VM) from .iso
- 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

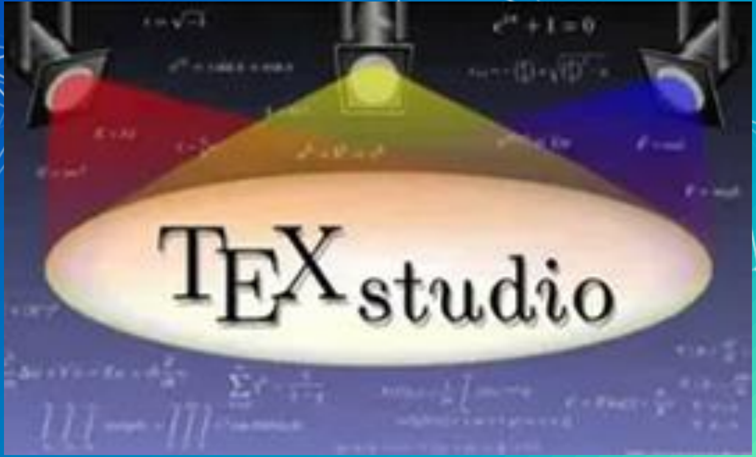
- Office hours (as posted on the https://ubnetdef.org/courses/syssec course page)
- General support in the Systems Security Mattermost channel
  - Subject to availability
  - Limited availability on Thursdays before class
- Open-Source Research
- Peer collaboration to achieve system state is acceptable

Weekly coursework components

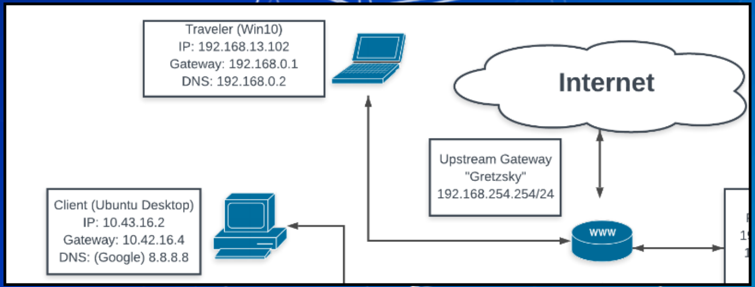
- Instructional Reports
    - Screenshots technical walk-through
- Requirements
    - Written professional report
- Topology
    - Visual network diagram
- A style guide for each component is in UB Learns

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
    - 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 Client 1: Windows 10
  - 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
  - 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 23.04
  - 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

- Welcome
  - Introduction
  - What is UBNetDef
- Class Overview
  - Learning outcomes
  - Course requirements
- CIATD
- Virtualization
  - In class exercise: Login to vCenter
  - In class exercise: Virtualization Activity
- Coursework
  - Workflow
  - Reporting
  - Topology
  - Assignment: Homework 1
    - In class exercise: Launch a new virtual machine (VM) from .iso
- 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 l**evel
- We did some virtualization
  - Accessed vSphere and launched a machine
- 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!