Welcome to Systems Security (SysSec)

System Security, Spring 2024
Week 1
Lead Presenter(s): SecDev

Opening Remarks

Featuring Prof. Cleary

Agenda – Week 1

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

Introductions

UB SecDev, Spring 2024

Raymond Harenza (**@rwharenz**)

Ethan Viapiano (**@ethanvia**)

Dikshit Khandelwal **(@dikshitkhandelwal)**

Lauren Moore **(@lbmoore)**

Steffi Yeh **(@cyeh4)**

Austin Chen **(@aechen2)**

Ben Juliano **(@bjjulian)**

Joshua Wajnryb **(@jwajnryb)**

Shreyas Ramesh **(@ramesh3)**

Overview - What is System Security?

This sets the stage for involvement with the hosting of:

- Camps
- Competitions
- Grantsmanship

As:

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

System Security Introductions

School of Management Faculty

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

Prof. Dominic Sellitto (@dsellitto)

Prof. David J. Murray (@djmurray)

Student Volunteers

Griffin Refol **(@grefol)**

Vasu Baldwa **(@vasudevb)**

Blake Turner **(@blaketnr)**

Alumni Volunteers

Phil Fox (@xphilfox)

Anthony Magrene **(@magrene)**

Stephen James (@stephenorjames)

Course Goals:

Learn, Have Fun, Be Your Best

Agenda – Week 1

- Welcome
  - Introduction
  - What is System Security
- 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

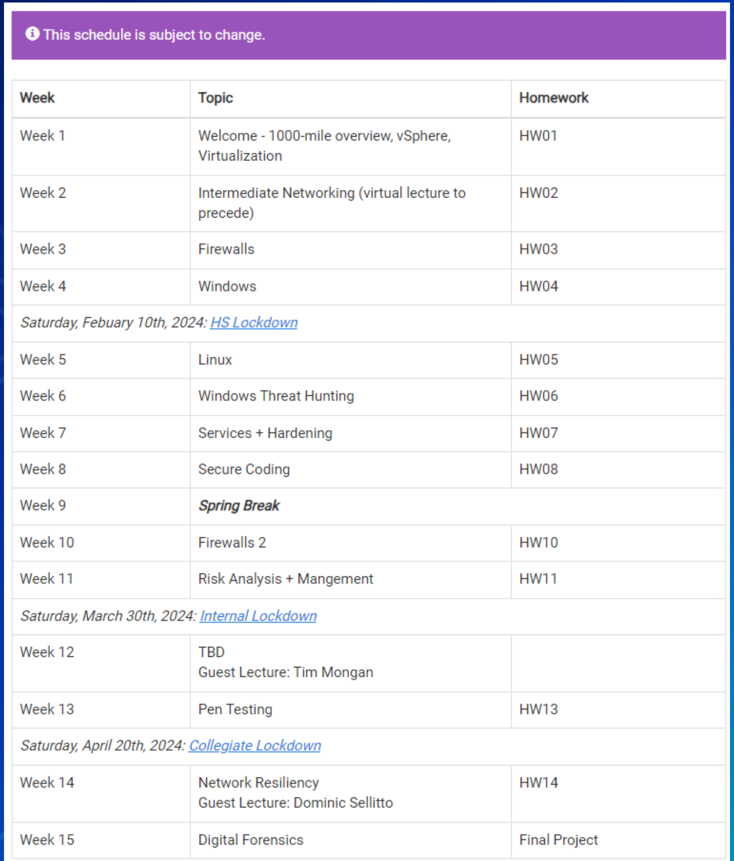
Learning Outcomes of This Class

- 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
- Everything covered in this class will be directly applicable to:
    - Homework assignments
    - In-class activites

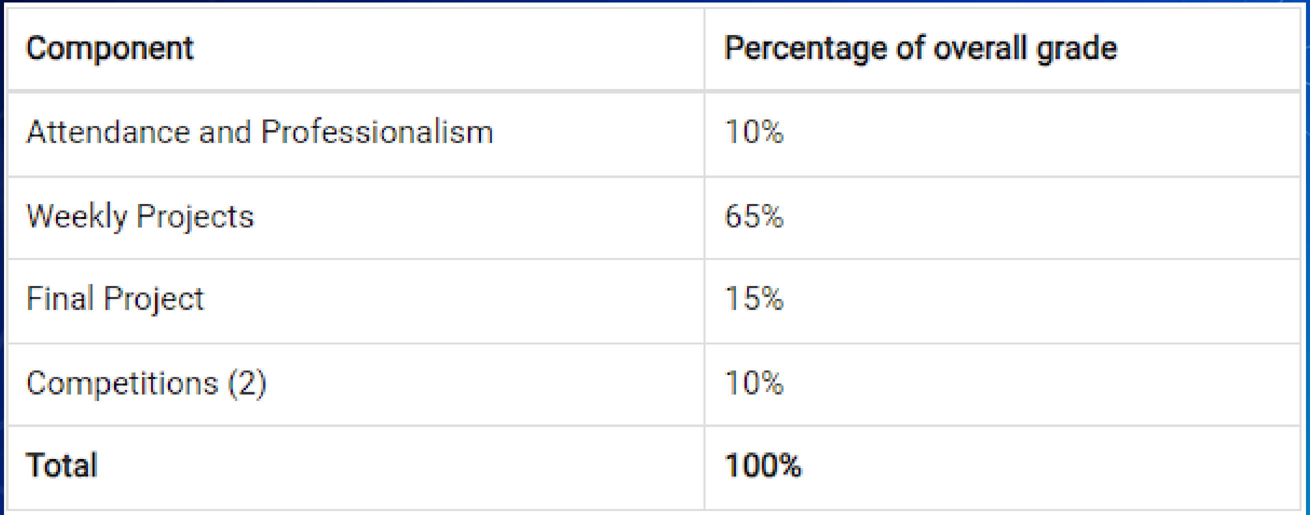
Tentative Class Schedule



ℹ This schedule is subject to change.

Week	Topic	Homework
Week 1	Welcome - 1000-mile overview, vSphere, Virtualization	HW01
Week 2	Intermediate Networking (virtual lecture to precede)	HW02
Week 3	Firewalls	HW03
Week 4	Windows	HW04
Saturday, Febuary 10th, 2024: HS Lockdown		
Week 5	Linux	HW05
Week 6	Windows Threat Hunting	HW06
Week 7	Services + Hardening	HW07
Week 8	Secure Coding	HW08
Week 9	***Spring Break***	
Week 10	Firewalls 2	HW10
Week 11	Risk Analysis + Mangement	HW11
Saturday, March 30th, 2024: Internal Lockdown		
Week 12	TBD Guest Lecture: Tim Mongan	
Week 13	Pen Testing	HW13
Saturday, April 20th, 2024: Collegiate Lockdown		
Week 14	Network Resiliency Guest Lecture: Dominic Sellitto	HW14
Week 15	Digital Forensics	Final Project

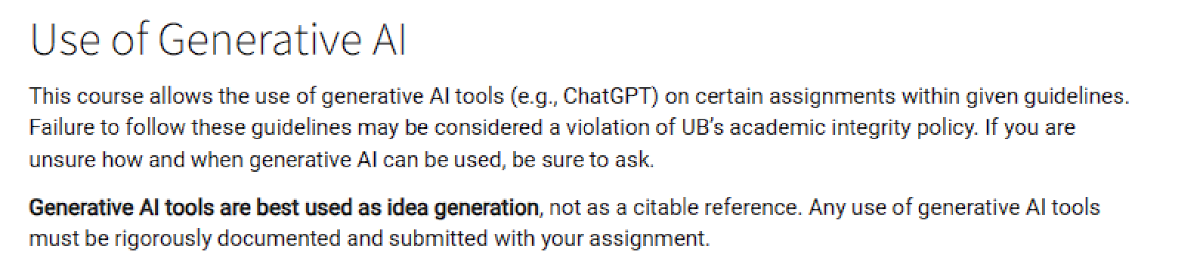
Course Requirements



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
- Generative AI



Use of Generative AI

This course allows the use of generative AI tools (e.g., ChatGPT) on certain assignments within given guidelines. Failure to follow these guidelines may be considered a violation of UB's academic integrity policy. If you are unsure how and when generative AI can be used, be sure to ask.

Generative AI tools are best used as idea generation, not as a citable reference. Any use of generative AI tools must be rigorously documented and submitted with your assignment.

Competitions!

- Highschool Lockdown February 10th
    - Contact @aderysh on Mattermost if you are interested
- UB Internal Lockdown
    - March 30th!
    - Sign up form: Will be provided in Mattermost when available
- External Competitions

Mattermost

- Go to:
  - https://chat.System Security.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 Spring 2024

Agenda – Week 1

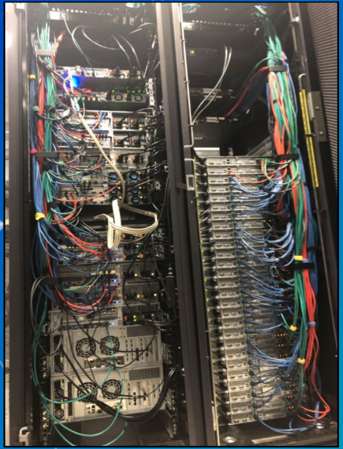
- Welcome
  - Introduction
  - What is System Security
- Class Overview
  - Learning outcomes
  - Course requirements
- CIATD
- Virtualization
  - In class exercise: Login to vCenter
  - In class exercise: Virtualization Activity
- Coursework
  - Workflow
  - Reporting
  - Topology
  - Assignment: Homework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

System Security Resources

As it turns out, System Security has you *all* covered already.

We have these:

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



Converging the analog: Virtualization

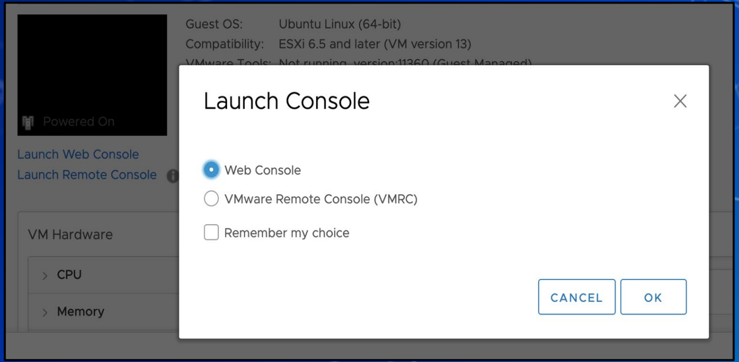
Instead, we’re going to get you the resources you need for this class through virtualization!

Explain Virtualization to your Mom

- 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

Virtualization: How do 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

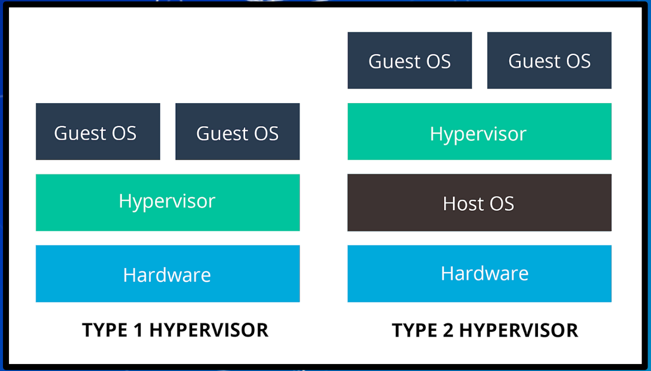
Launch Console

● Web Console

○ VMware Remote Console (VMRC)

□ Remember my choice

Use case of virtualization



- Type 1
  - Bare Metal Hypervisors access machine resources directly. (SysSec Version)
- Type 2
  - Hosted Hypervisors run on an underlying operating system, and are given resources for guests to use by the host. (Other courses)

Type 2 Virtualization

- Intel/AMD Hosts
  - Can utilize software like VirtualBox
- Apple Silicon Hosts
  - Must utilize ARM ISO’s and software such as Qemu or UTM

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://System Security.org/courses/syssec/
    - Also available on UBLearns!
  - Favorite/Bookmark vCenter!

Break slide

Please return on time!

Agenda – Week 1

- Welcome
  - Introduction
  - What is System Security
- 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 (Bright Space)
  - Required .pdf format uploads
    - **Will not be graded if not in .pdf format**
- Notes will be posted at https://ubnetdef.org/lectures/
- Class work will correspond to the homework
  - Pay attention in class
  - Complete the in class activates

SysSec Homework

- Reports
  - Instruction report
  - Informational report
- 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**

Report components

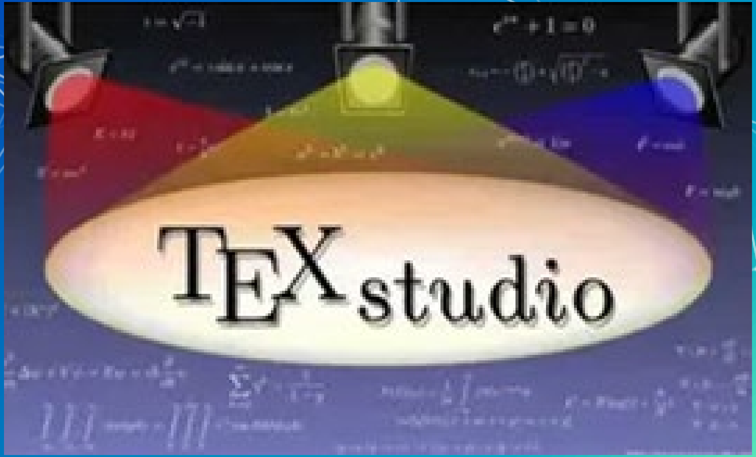
- Instructional Reports
  - Screenshots technical walk-through
- Informational reports
  - Inform select audiences
- Requirements
  - Written professional report
- Topology
  - Visual network diagram
- A style guide for each component is in UB Learns

Coursework Support

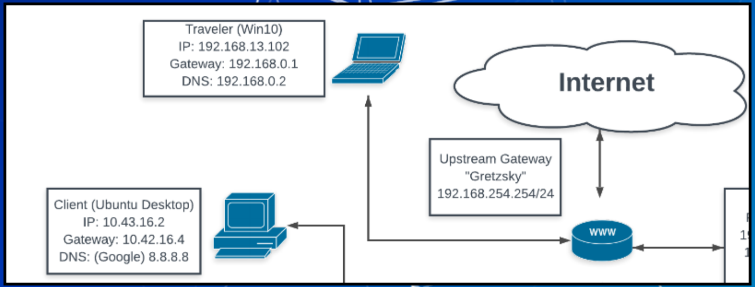
- Office hours (as posted on the https://System Security.org/courses/syssec course page)
- General support in the Systems Security Mattermost channel
  - Subject to availability
  - Limited availability on Thursdays before class
  - Consult this resource to improve support timeliness: https://nohello.net/en/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

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.



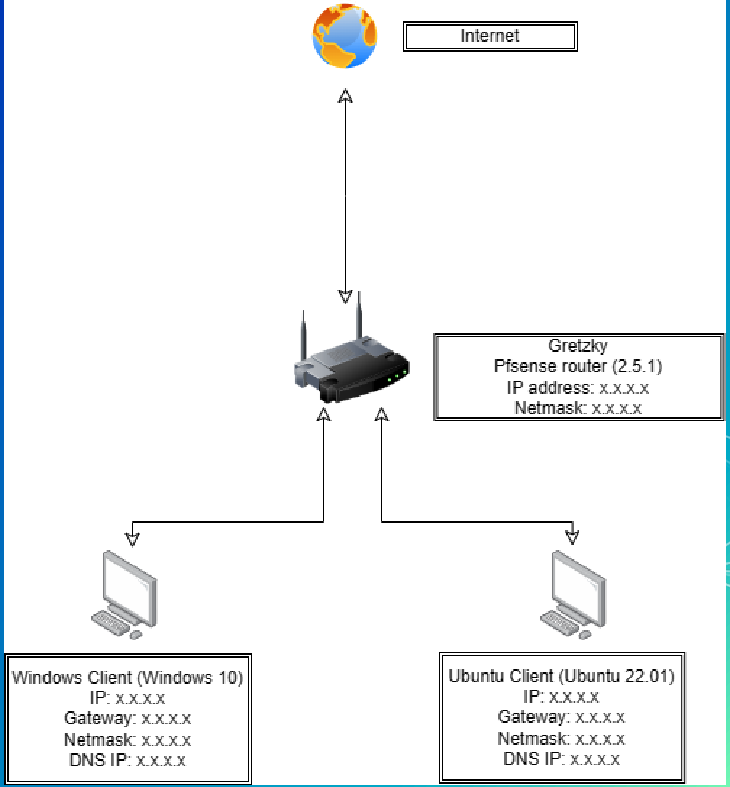
Common coursework component: Topology



- 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

Open up topology style guide and go over it in depth

- Provides layout and general guidelines for topologies
- Key pointers:
  - System information
  - Connection flow
  - Hierarchical system placement



Internet

Gretzky
Pfsense router (2.5.1)
IP address: x.x.x.x
Netmask: x.x.x.x

Windows Client (Windows 10)
IP: x.x.x.x
Gateway: x.x.x.x
Netmask: x.x.x.x
DNS IP: x.x.x.x

Ubuntu Client (Ubuntu 22.01)
IP: x.x.x.x
Gateway: x.x.x.x
Netmask: x.x.x.x
DNS IP: x.x.x.x

In Class Activity

Network Topology Walkthrough

Creating a Network Topology

- In diagrams.net:
  - Open a new diagram
  - Click on + More Shapes
  - Select one of the following
    - Clipart, Cisco19, Citrix
  - Click on Apply
  - Expand your selection from the dropdown list
  - Drag and drop the figures corresponding to their device
  - Connect each device with an arrow indicating the flow of network traffic
  - Select a Rectangle to label each network device
  - See the Topology Style Guide for more details

List of devices to be included on the topology:

Name (network devices)	Operating System	IP
DemoRouter	pfSense 2.7.2	74.110.50.221
interface1		172.16.0.1/26

Name (endpoints)	Operating System	IP	Subnet Mask	DNS	Default Gateway
DemoClientA	Ubuntu 23.10	172.16.0.10	255.255.255.192	8.8.8.8	172.16.0.1
DemoClientB	Windows 10	172.16.0.20	255.255.255.192	8.8.8.8	172.16.0.1

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 23.10.1
  - All usernames and passwords must match:
    - `sysadmin`
    - `Change.me!`
- Perform simple network tests on each using the Command-Line Interface (CLI). Take screenshots!
- System state: Both client installations are complete and are network-connected.
- Provide a topology of your network

Instructional Report Style Guide Introduction/overview

- Provides layout and general guidelines for homework
- Key pointers:
  - Screenshots
  - Page layout
  - In-paragraph organization
  - Punctuation and grammar

Agenda – Week 1

- Welcome
  - Introduction
  - What is System Security
- 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 System Security is
- 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

Questions

Now is the time!

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 <u>`Edit Settings...`</u>
  - Scroll down to <u>`CD/DVD drive 1`</u>
  - From the drop down select <u>`Datastore ISO File`</u>
  - Select <u>`cdr-iscsi1`</u>
  - Scroll down to <u>`ISOs`</u>
  - Select either a Windows or Linux ISO. Consult HW for the name.
  - Click <u>OK</u> and make sure the connected option is checked

Class dismissed

See you next week!