Welcome to Systems Security (SysSec)

UBNetDef, Spring 2021

Week 1

Lead Presenter: Phil Fox

Special Thanks: Anthony Magrene, Stephen James

Agenda - Week 1

1. Welcome
   - 1.1. Introductions
   - 1.2. Opening remarks
   - 1.3. Ground rules
2. Overview
3. Virtualization
   - 3.1. In Class exercise: Go Virtualize
4. Coursework
   - 4.1. Workflow
   - 4.2. Support
   - 4.3. Reporting
   - 4.4. Topology
     - 4.4.1. In class exercise: Develop a topology diagram
   - 4.5. Assignment: Homework 1
     - 4.5.1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up

Introductions

UB SecDev, Spring 2021

Phil Fox (@xphilfox) - SecDev Lead, UB CCDC

Shreya Lakhkar (@shreya) - F20 SecDev Lead, CCDC

Anthony Magrene (@magrene) - Lockdown Red Team Lead, CCDC, CPTC

Aibek Zhylkaidarov (@aibek) - UBNetDef Infrastructure Support, F20 CCDC

Orly Stein (@orlystei) - Lockdown Red Team, CCDC, CPTC

Michael Morgenthal (@mmorgent) - Lockdown White Team, UBNetDef Webmaster

Nick Richter (@nickrichter) - Lockdown White Team

Introductions

UB NetDef Faculty

Prof. David J. Murray (@djmurray)

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

UB SecDev Alumni Volunteers

Prof. Dominic Sellitto (@dsellitto)

Stephen James (@stephenorjames)

Aaron Fiebelkorn (@aaron)

Nick Brase (@nickbrase)

Jay Chen (@jay_c)

Chris Klimek (@chrisklimek)

UB SecDev Student Volunteer Staff

Aritra Paul (@aritra)

Andrew Hu (@ahu5)

Anna Lisske (@alisske)

Ed Christian (@christi6) - White Team Lead

Gursimran Singh (@gursimr2)

Jack Lynch (@edwardly)

Jackie Dufresne (@jldufres)

Ruben Ocana (@ruben_ocana)

Vasu Baldwa (@vasudev) - Black Team Lead

*Indicates an S21 lead instructor role

Opening Remarks

Featuring Prof. Murray

UBNetDef Goals:

Learn, Have Fun, Be Your Best

Ground Rules

- Lectures: Recorded for archive (starting now!)
- Cameras: Keep on for all learners and active presenters during class time
  - Prepare for requests for thumbs-up!
  - Does this make sense? (Demo)
- In-class Q&A: On-mic unless *otherwise* specified
  - E.g., ‘answer 1,2,3’ in the chat, polls, etc.
  - Share the conversation
  - Grow your trust with the group; courage > ‘correctness’
- Text chat: Help keep it readable for instruction materials, links, etc.
- Attendance: Taken weekly during lecture time
- Homework: Weekly, deliverables due Thursdays 7:04(:59) pm

Agenda - Week 1

1. Welcome
   - 1.1. Introductions
   - 1.2. Opening remarks
   - 1.3. Ground rules
2. Overview
3. Virtualization
   - 3.1. In Class exercise: Go Virtualize
4. Coursework
   - 4.1. Workflow
   - 4.2. Support
   - 4.3. Reporting
   - 4.4. Topology
     - 4.4.1. In class exercise: Develop a topology diagram
   - 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)

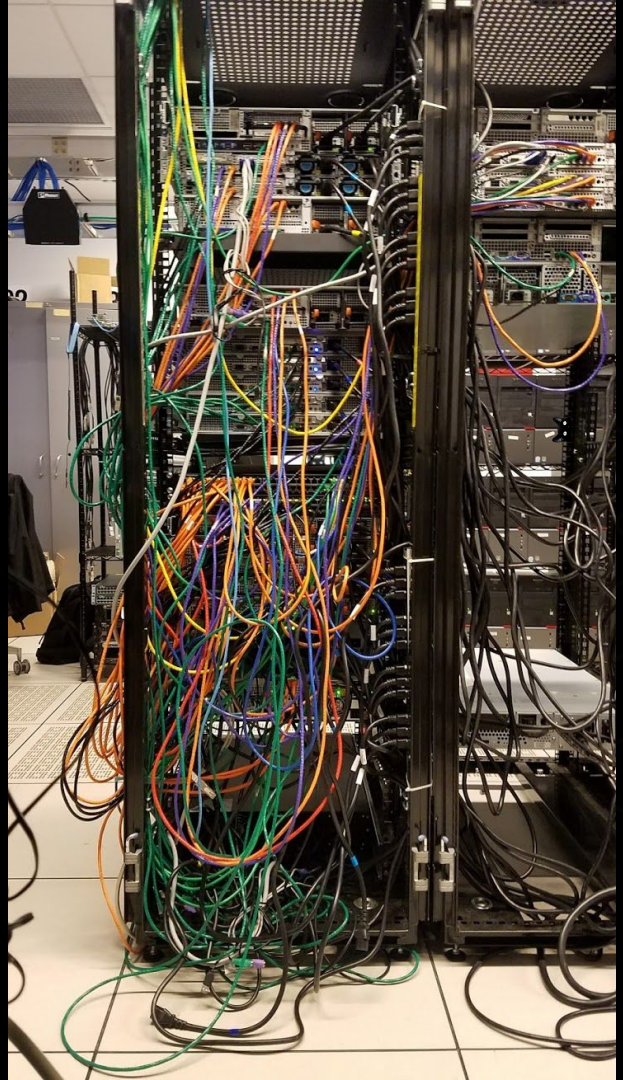
Overview - UBNetDef Learners

The (for-credit!) courses

- SysSec: The gateway
- Network Security (NetSec)
  - Linux software and networking deep dive
  - Packet analysis
- Scripting Security (I will always call this 'ScripSec' whether it catches on or not)
  - Bash programming
  - Security project
- Security Development (SecDev)
  - Course and curriculum development/instruction
  - Infrastructure management (behind the scenes preview next!)

An MBA and two CSE students walk into a server room...

leaves



...only one

NetDef

001

011

010

#WorkingTogether

NetDef

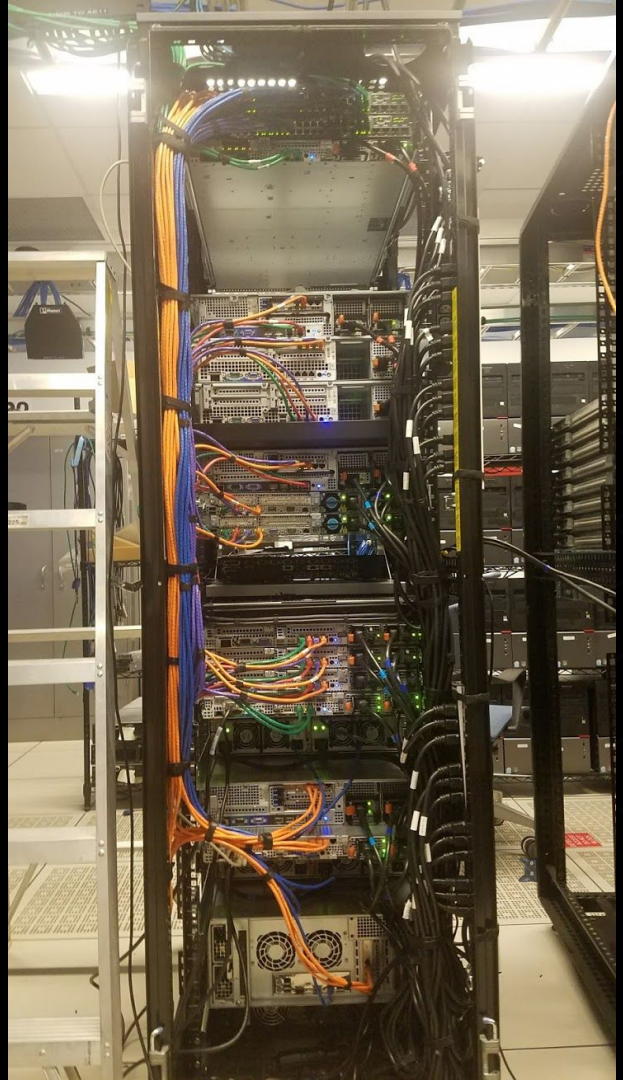
001

011

010


SECURITY


04

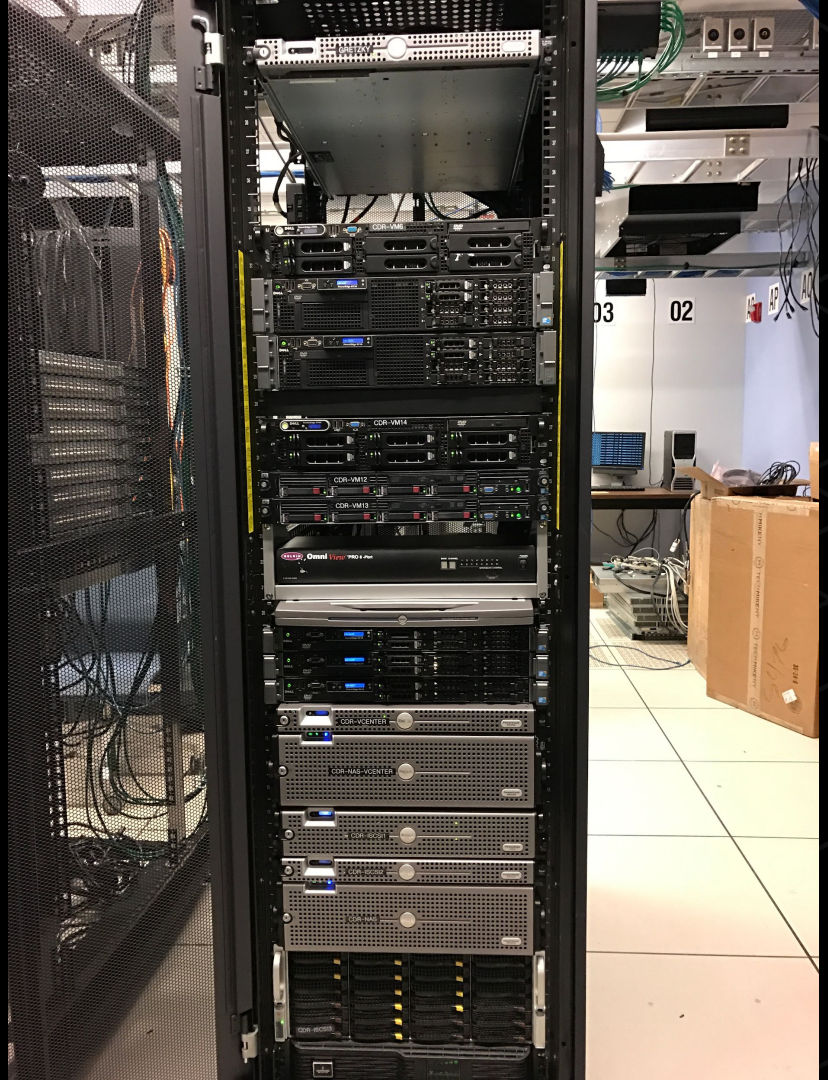


NetDef

001

011

010



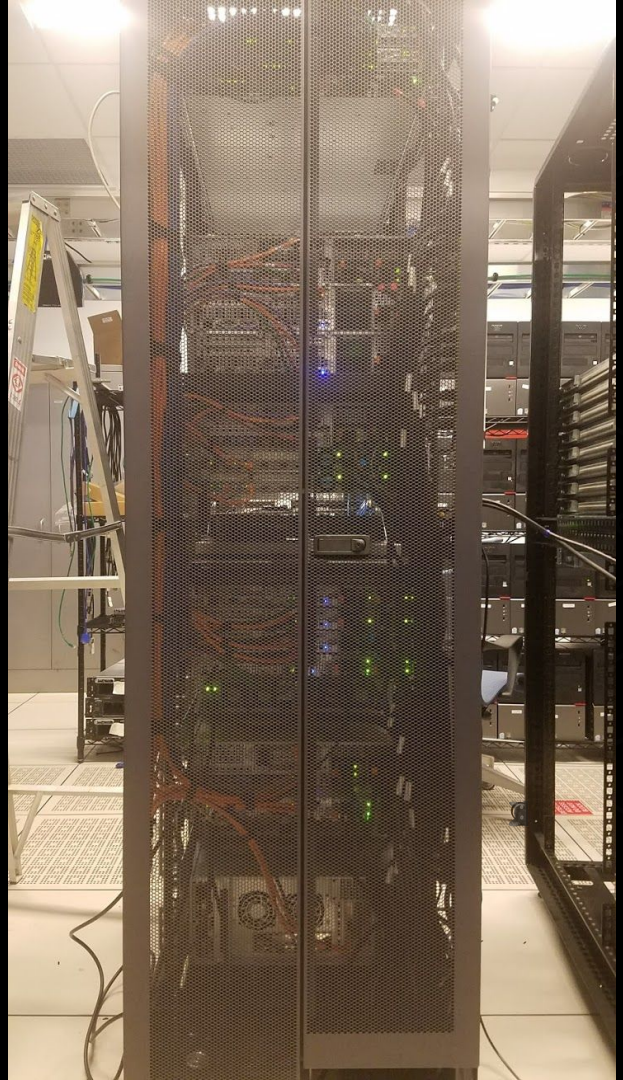
NetDef

001

011

010

THE DOORS CAN CLOSE!!!

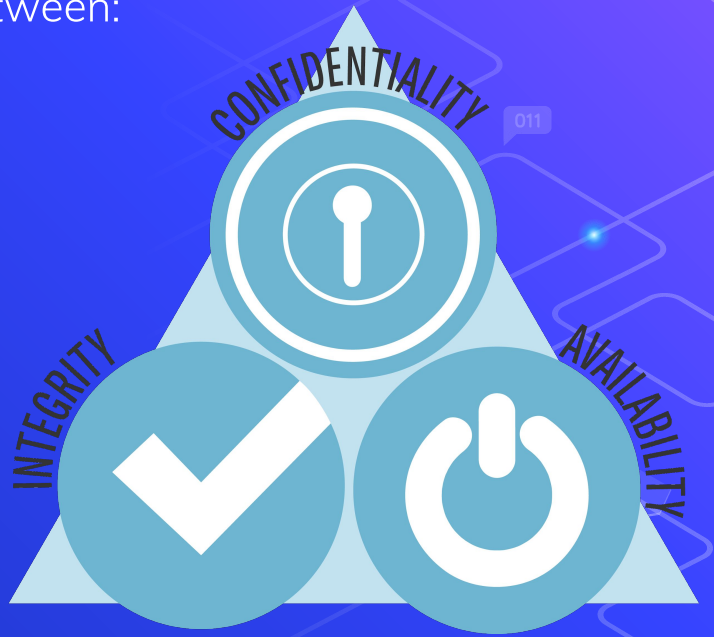


BOTH OF THEM!!!!!

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”

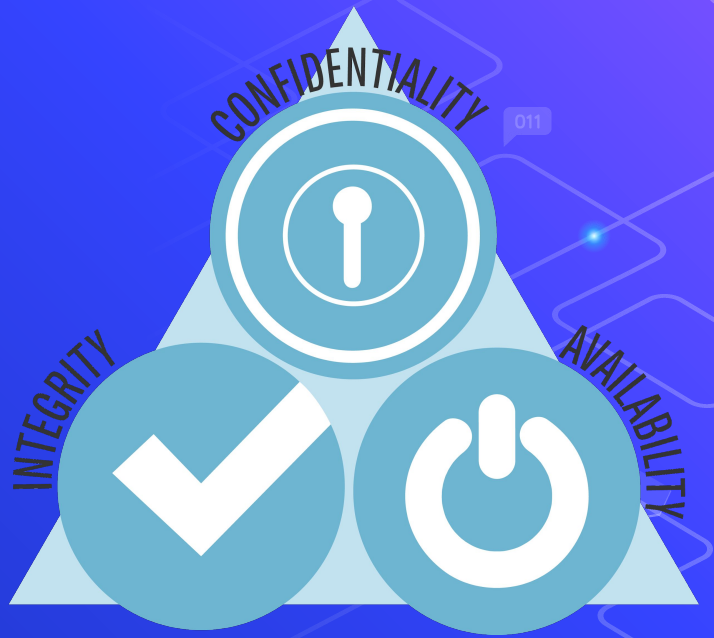


Overview - Cybersecurity

Discussion (roundtable):

What's the difference?

- Confidentiality
- Availability
- Integrity



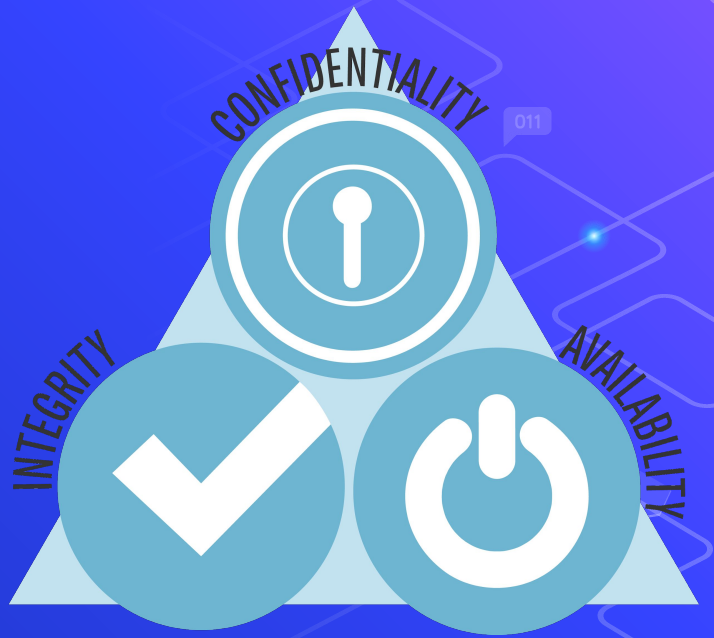
Overview - Cybersecurity

Discussion (roundtable):

What's the difference?

- Confidentiality
- Availability
- Integrity

Which is most important?



Overview - Cybersecurity

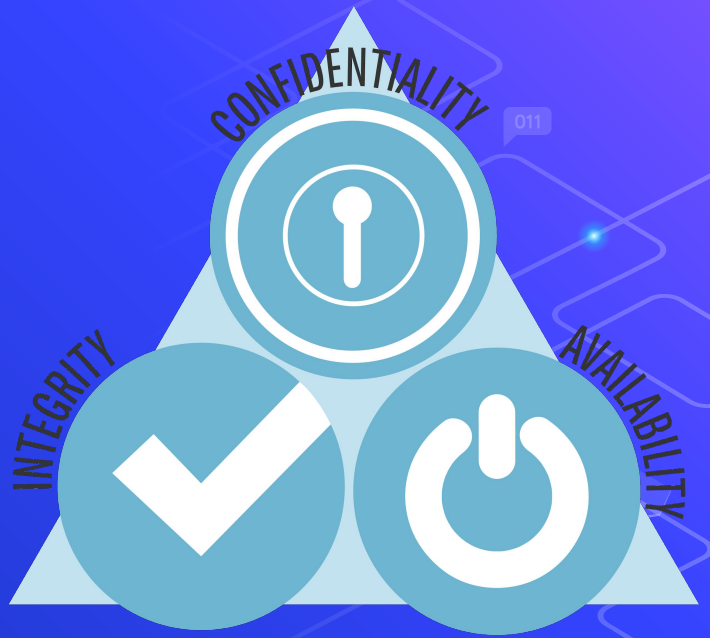
Discussion (roundtable):

What's the difference?

- Confidentiality
- Availability
- Integrity

Which is most important?

Can priorities between the three change?



Overview - Cybersecurity

Discussion (roundtable):

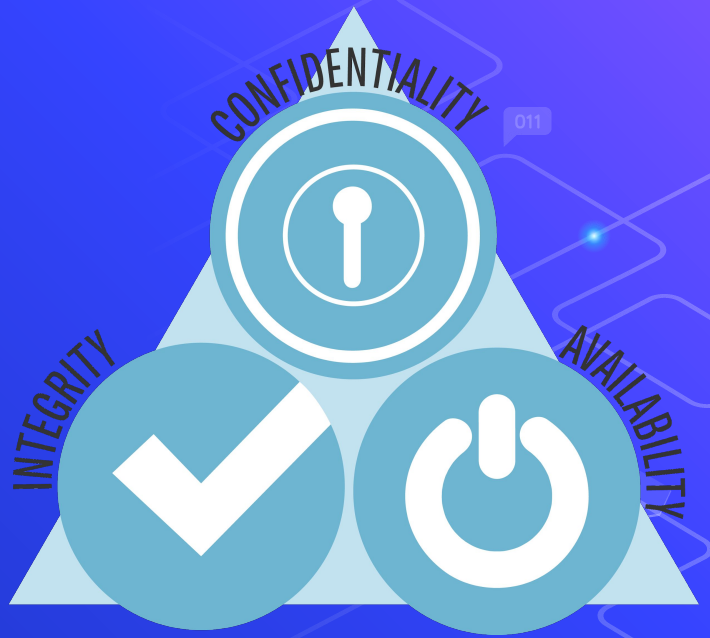
What's the difference?

- Confidentiality
- Availability
- Integrity

Which is most important?

Can priorities between the three change?

Challenge: Subdivide one pillar



Overview - Cybersecurity Roles

Discussion (roundtable):

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
2. Overview
3. Virtualization
   - 3.1. In Class exercise: Go Virtualize
4. Coursework
   - 4.1. Workflow
   - 4.2. Support
   - 4.3. Reporting
   - 4.4. Topology
     - 4.4.1. In class exercise: Develop a topology diagram
   - 4.5. Assignment: Homework 1
     - 4.5.1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up

An analogous scenario: Zoom outage!

You are in the middle of a Zoom call and it disconnects

Discuss (roundtable): What do you do?

An analogous scenario: A class on Zoom outages

Good. You are clearly experts...

...so much so that you will instruct the class: MIS 099 My Internet Is Down

We have to develop the syllabus, namely the required course materials!

Discuss: What will students need for their remote labs?

An analogous scenario: A class on Zoom outages

Good. You are clearly experts…

…so much so that you will instruct the class: MIS 099 My Internet Is Down

We have to develop the syllabus, namely the required course materials!

Discuss: What will students need for their remote labs?

Discuss: (About) how much would that cost?

An analogous scenario: A class on Zoom outages

Good. You are clearly experts…

…so much so that you will instruct the class: MIS 099 My Internet Is Down

We have to develop the syllabus, namely the required course materials!

Discuss: What will students need for their remote labs?

Discuss: (About) how much would that cost?

Discuss: Knowing what we now know, would anybody take our class?

An analogous scenario: Course materials

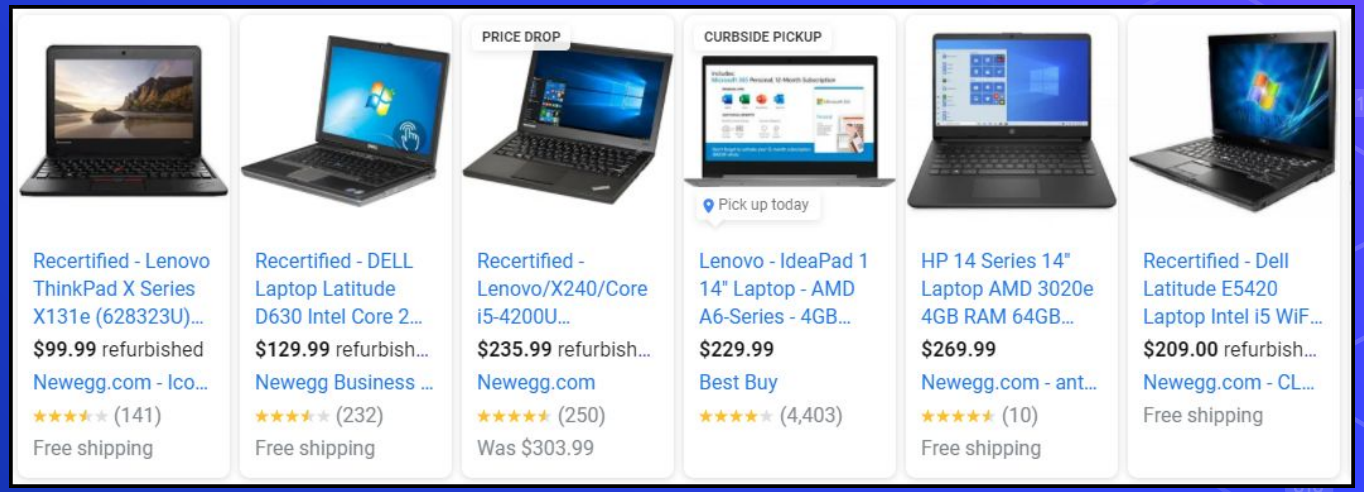
Now, imagine that we (SecDev) actually forgot to put the required materials for this class on the syllabus. Here's what we're looking at:

Cabling and utility charges:

Good enough internet: **$85**+/mo.
Uptime (electric): ~**$20**/mo.
Cooling (electric): ~**$20**/mo.

An analogous scenario: Course materials

Additional clients (3):



An analogous scenario: Course materials

Windows 10 and Server licensing:

An analogous scenario: Course materials

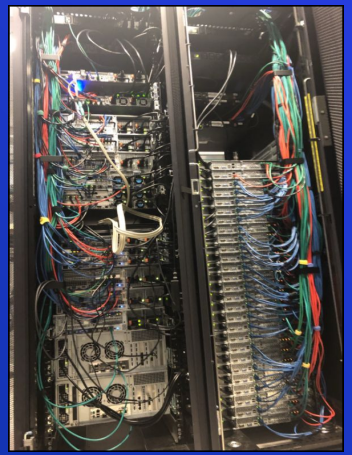
Webservers (3):

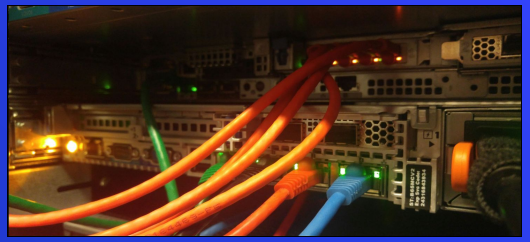
An analogous scenario: UBNetDef resources

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.





(Just kidding)

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, as you observe

Virtualization: Let's look inside

- Login to vCenter
  - Primary course links available at https://ubnetdef.org/courses/syssec/
    - Also available on UBLearns!
  - vCenter: http://cdr-vcenter.cse.buffalo.edu/
  - Use your full UB email for the login ID
- Let's split into breakout rooms and get logged in!

Breakout Groups Assignments

- We have teams sorted for this week's lecture!
- Team 1 (Shreya):
  - Cameron, Shaz, Hannah, Aiden
- Team 2 (Anthony):
  - Chris, Radhika, Devin, Steve
- Team 3 (Orly):
  - Ben, Anthony, J, Mike
- Team 4 (Vasu):
  - Ahssan, Matt, Alain

Virtualization: Let's look inside

- Login to vCenter
  - Primary course links available at https://ubnetdef.org/courses/syssec/
    - Also available on UBLearns!
  - vCenter: http://cdr-vcenter.cse.buffalo.edu/
  - Use your full UB email for the login ID

Breakout 01

Login to vCenter

Virtualization: Let's look inside

- Login to vCenter
  - Primary course links available at https://ubnetdef.org/courses/syssec/
    - Also available on UBLearns!
  - vCenter: http://cdr-vcenter.cse.buffalo.edu/
  - Use your full UB email for the login ID
- Check it out: You have a device!

Virtualization: Let's look inside

- Login to vCenter
  - Primary course links available at https://ubnetdef.org/courses/syssec/
    - Also available on UBLearns!
  - vCenter: http://cdr-vcenter.cse.buffalo.edu/
  - Use your full UB email for the login ID
- Check it out: You have a device!
- Oh no…
  - Let's take a break so I can sort this one out.

Break slide

Please return on time!

Your machine: Operation

- It serves web page data to other devices on the network
  - It's a "webserver"
- You can't exactly see the page itself, but other devices can
  - Those with *graphic* user interfaces (GUIs) unlike your *command line* interface (CLI)
- Our records show, the hosted webpage *used* to look like this:

Your machine: Current state

First, let's take a look together.

Hmm....

We need to investigate what happened

Breakout rooms

- With your SecDev mentor find out:
  - Who did it?
  - When this happened
  - How this was possible
  - What we can do to fix it
    - I.e., where the defaced files are
- Elect a group representative
- The group representative shares their findings with the class

Breakout 02

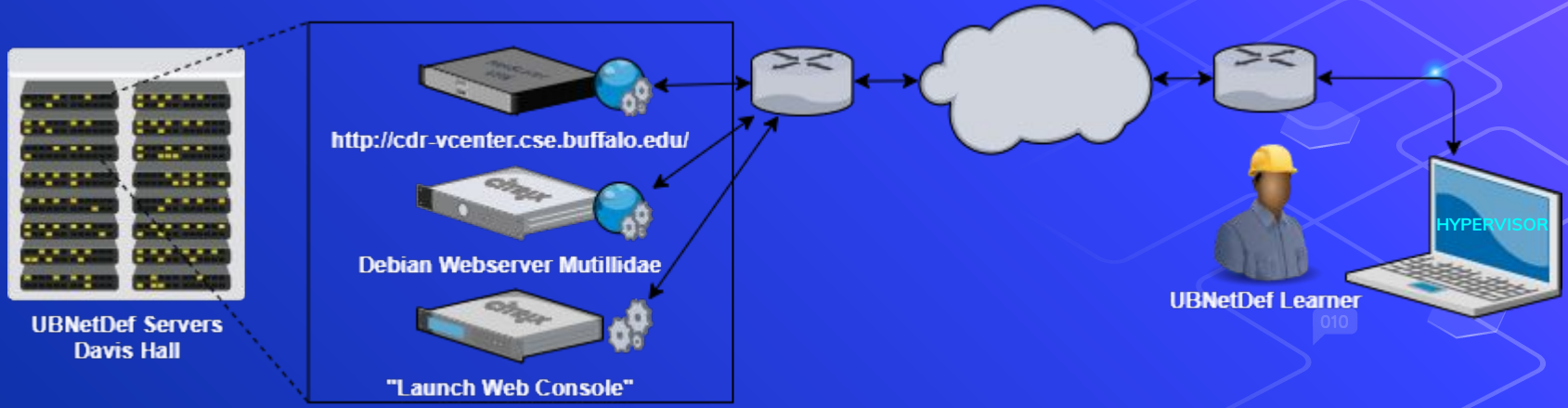
Incident Response

What did we uncover?

- When did the attack occur?
- How did the attacker gain access?
- Who was the attacker?
  - Which IP address?
  - Which local account?
- What can we do to fix it?

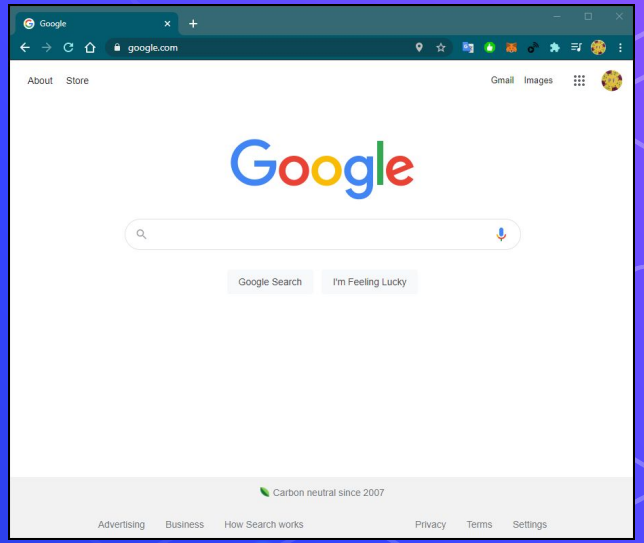
Back to virtualization: How did we do that?

- Servers serving services!
- Not just webpages, but entire devices!
- Not just entire devices, but a hypervisor that lets learners interact with devices!



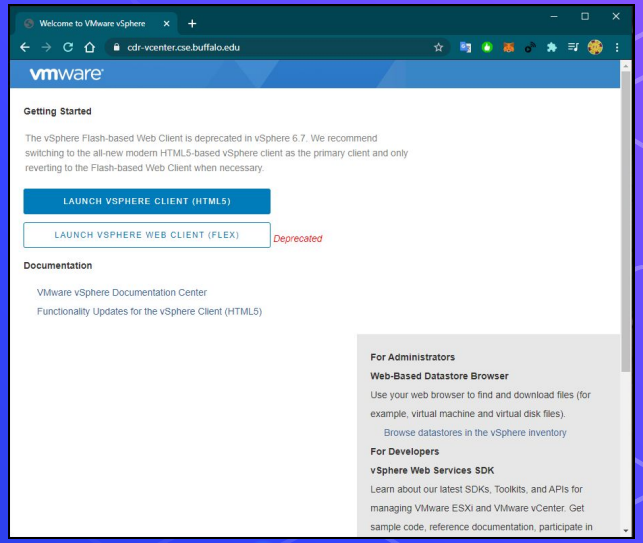
Virtualization: What (you) the end user sees

- **Host machine launches a browser**
- The browser GETs the vCenter webpage
- The vCenter webpage lists virtual devices
- The vCenter webpage launches a hypervisor
- The hypervisor allows end users to interact:
  - Using the host I/O (monitor, mouse, keyboard)
  - Through the browser (web)
  - To the console of a virtual device!



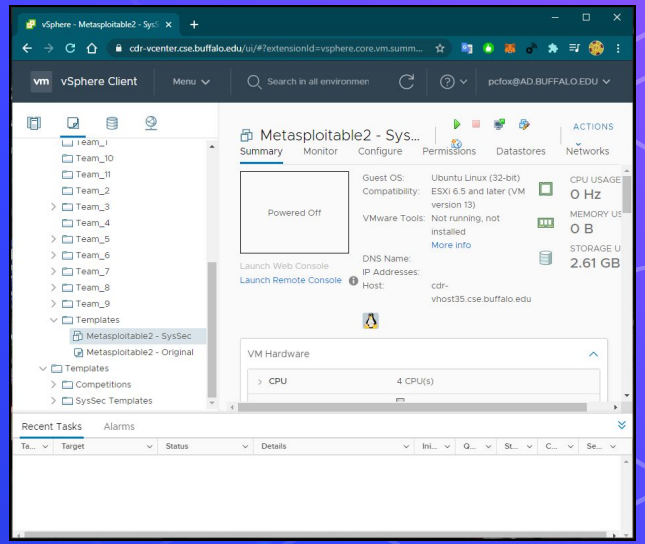
Virtualization: What the end user sees

- Host machine launches a browser
- **The browser GETs the vCenter webpage**
- The vCenter webpage lists virtual devices
- The vCenter webpage launches a hypervisor
- The hypervisor allows end users to interact:
  - Using the host I/O (monitor, mouse, keyboard)
  - Through the browser (web)
  - To the console of a virtual device!



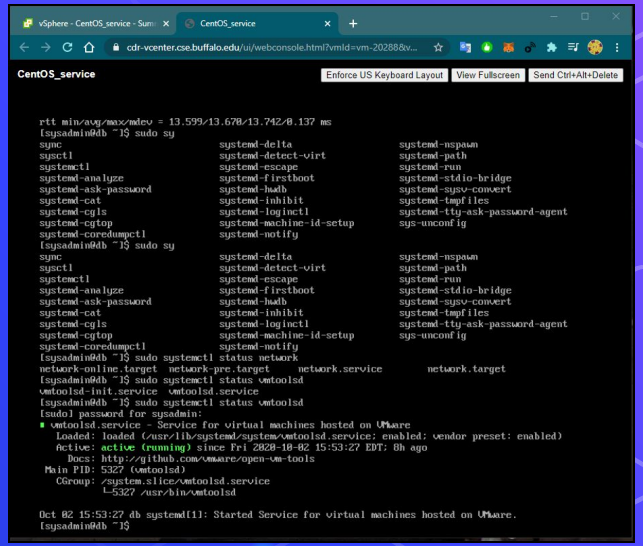
Virtualization: What the end user sees

- Host machine launches a browser
- The browser GETs the vCenter webpage
- **The vCenter webpage lists virtual devices**
- The vCenter webpage launches a hypervisor
- The hypervisor allows end users to interact:
  - Using the host I/O (monitor, mouse, keyboard)
  - Through the browser (web)
  - To the console of a virtual device!



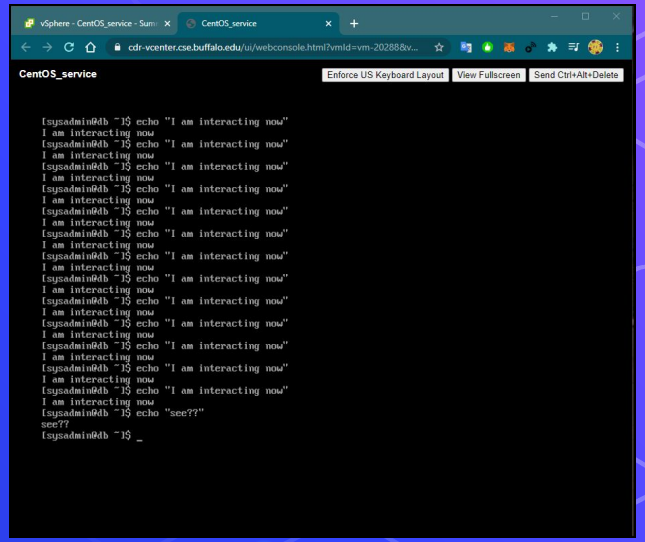
Virtualization: What the end user sees

- Host machine launches a browser
- The browser GETs the vCenter webpage
- The vCenter webpage lists virtual devices
- **The vCenter webpage launches a hypervisor**
- The hypervisor allows end users to interact:
  - Using the host I/O (monitor, mouse, keyboard)
  - Through the browser (web)
  - To the console of a virtual device!



Virtualization: What the end user sees

- Host machine launches a browser
- The browser GETs the vCenter webpage
- The vCenter webpage lists virtual devices
- The vCenter webpage launches a hypervisor
- **The hypervisor allows end users to interact:**
  - Using the host I/O (monitor, mouse, keyboard)
  - Through the browser (web)
  - To the console of a virtual device!



Break slide

Please return on time!

Agenda - Week 1

1. Welcome
   - 1.1. Introductions
   - 1.2. Opening remarks
   - 1.3. Ground rules
2. Overview
3. Virtualization
   - 3.1. In Class exercise: Go Virtualize
4. Coursework
   - 4.1. Workflow
   - 4.2. Support
   - 4.3. Reporting
   - 4.4. Topology
     - 4.4.1. In class exercise: Develop a topology diagram
   - 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

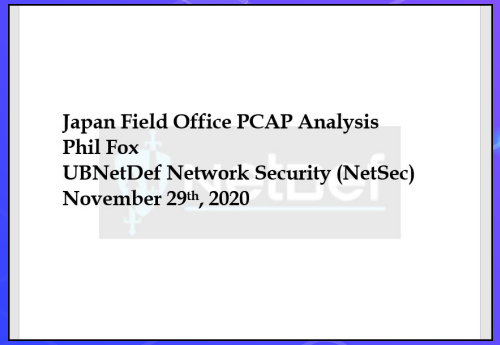
- Assigned weekly
- Delivery and turn-in via UBLearns
  - Required .pdf format uploads
- Select weeks: System state
  - Scored separate of report deliverable
  - Remediation required
- Due the subsequent **Thursday, 7:04:59 pm**
- Almost strictly compliments lecture
  - Take good notes in-class!

Coursework Support

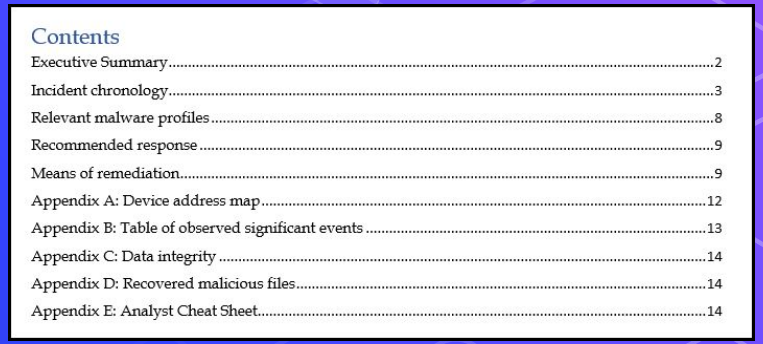
- Office hours (as posted on the https://ubnetdef.org course page)
  - Phil - Wednesdays, 5:30p
  - Shreya - Thursdays, 2p
  - Anthony - Saturdays, 11a
  - Aibek - Fridays, 6p
  - Orly - Thursdays, 10a
  - Mike - Tuesdays, 10a
  - Nick - Mondays, 12p
- General support in the Systems Security Mattermost channel
  - Subject to availability

Weekly coursework component: Reports

- Requirements
  - **Academic header or title page**
  - Table of contents (if more than 2 content pages)
  - Proper grammar and spelling
  - Instructional reports/report segments
    - Screenshots and descriptions supporting all pertinent steps
    - Note: Audience is not familiar with the systems in question
  - Informational reports/report segments
    - Citations
      - Consistent academic standard (e.g., MLA, IEEE)
      - Per-page in footer -or-
      - References/works cited page


Japan Field Office PCAP Analysis
Phil Fox
UBNetDef Network Security (NetSec)
November 29th, 2020

Weekly coursework component: Reports


Contents

- Requirements
  - Academic header or title page
  - **Table of contents** (if more than 2 content pages)
  - Proper grammar and spelling
  - Instructional reports/report segments
    - Screenshots and descriptions supporting all pertinent steps
    - Note: Audience is not familiar with the systems in question
  - Informational reports/report segments
    - Citations
      - Consistent academic standard (e.g., MLA, IEEE)
      - Per-page in footer -or-
      - References/works cited page

Weekly coursework component: Reports

- Requirements
  - Academic header or title page
  - Table of contents (if more than 2 content pages)
  - Proper grammar and spelling
  - **Instructional reports/report segments**
    - **Screenshots and descriptions supporting all pertinent steps**
    - Note: Audience is not familiar with the systems in question
  - Informational reports/report segments
    - Citations
      - Consistent academic standard (e.g., MLA, IEEE)
      - Per-page in footer -or-
      - References/works cited page

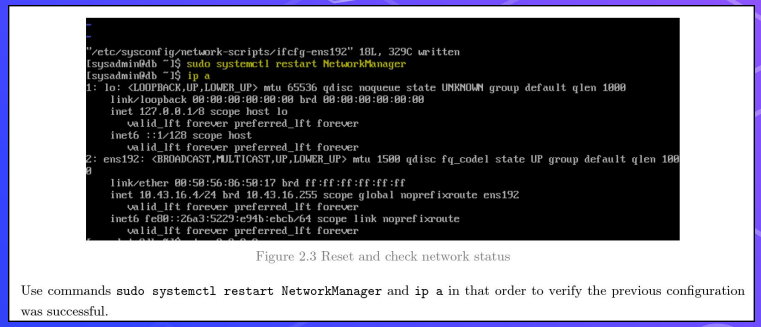
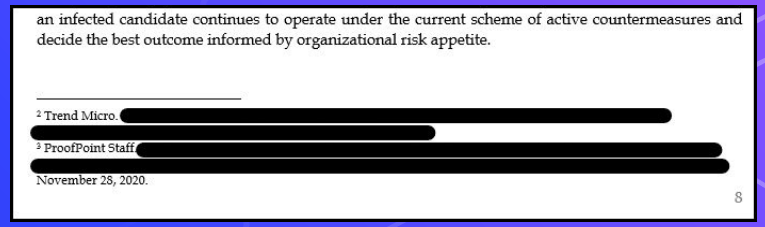


Figure 2.3 Reset and check network status

Use commands `sudo systemctl restart NetworkManager` and `ip a` in that order to verify the previous configuration was successful.

Weekly coursework component: Reports

- Requirements
  - Academic header or title page
  - Table of contents (if more than 2 content pages)
  - Proper grammar and spelling
  - Instructional reports/report segments
    - Screenshots and descriptions supporting all pertinent steps
    - Note: Audience is not familiar with the systems in question
  - **Informational reports/report segments**
    - **Citations**
      - Consistent academic standard (e.g., MLA, IEEE)
      - Per-page in footer -or-
      - References/works cited page


an infected candidate continues to operate under the current scheme of active countermeasures and decide the best outcome informed by organizational risk appetite.

[2] Trend Micro, [redacted]

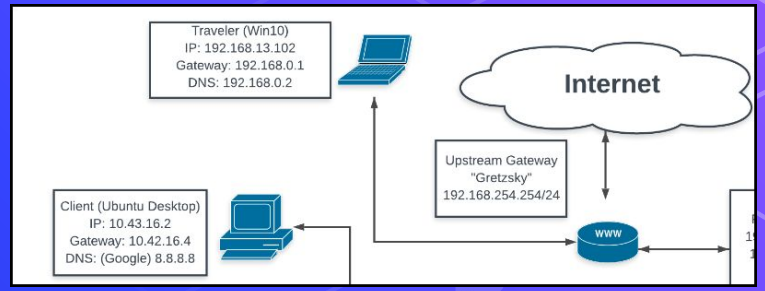
[3] ProofPoint Staff, [redacted]

November 28, 2020.

8

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
  - All devices represented as if physically available
  - Device details correspond exactly to system states



Common coursework component: Topology

- We're serious about topologies; so much so, that we're doing one together!
- Indicate:
  - The infected device
  - The gateway that it is connected to
  - The web
  - The attacker
    - [ ] Can we tell how they're connected to our infected device?

Breakout 03

Build a topology

Common coursework component: Remediation

- 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.
  - Aiming for end-of-lecture (i.e., a 3 hr. turnaround)
- 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.
  - Early-cycle office hours: Aibek (Fri. 6p), Anthony (Sat. 11a)

Homework 1 (HW01)

- Posted to UBLearns by 10 pm
- Install two clients from .iso on your network segment/vCenter folder
  - Client 1: Windows 10
  - Client 2: Ubuntu Linux Desktop version 18.04 (Bionic)
  - All usernames and passwords must match:
    - `sysadmin`
    - `Change.me!`
- Perform simple network tests on each using the CLI. Take screenshots!
- Update your existing topology to include these two new devices connected on the same gateway.
  - Include the topology in your report body
- System state: Both client installations are complete and are network-connected.

Breakout rooms: Launch a VM from .iso

- In vCenter with your breakout room mentor:
  - Choose the less familiar operating system in the prior slide
  - One brave volunteer share your screen
  - Follow your mentor's instructions on how to launch an .iso!

Breakout 04

Launch a new VM from ISO

Agenda - Week 1

1. Welcome
   - 1.1. Introductions
   - 1.2. Opening remarks
   - 1.3. Ground rules
2. Overview
3. Virtualization
   - 3.1. In Class exercise: Go Virtualize
4. Coursework
   - 4.1. Workflow
   - 4.2. Support
   - 4.3. Reporting
   - 4.4. Topology
     - 4.4.1. In class exercise: Develop a topology diagram
   - 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 cybersecurity at a **high** level
- We did some virtualization
  - Incident response
  - Launch a machine
- We communicated the standards for reporting
  - We built a topology
- We described the homework process, this week's HW, and course resources

Parting questions

Now is the time!

Don’t leave (yet)! Reasons to stay after:

- High School Lockdown v5
  - Pre-competition information
  - White team meeting!
- Homework break-outs available
  - An early start gives you a huge edge on timely completion
  - Good time to address feedback for remediation when necessary

Class dismissed

See you Saturday or next week!