

# Welcome to Systems Security (SysSec)

UBNetDef, Fall 2021

Week 1

Lead Presenter: Radhika Jois

Special Thanks: Phil Fox

# 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
  - 4.5. Field Trip: Data Center
  - 4.6. Assignment: Homework 1
    - 4.6.1. In class exercise: Launch a new Virtual Machine (VM) from .iso
5. Summary/Wrap-up

# Mattermost

# Introductions

UB SecDev, Fall 2021

Radhika Jois (**@radhikaj**) - SecDev Lead, White Team Lead, CCDC

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

Vasudev Baldwa (**@vasudevb**) - Infrastructure/Lockdown Black Team Lead, CCDC, CPTC

Lucas Crassidis (**@luke**) - Lockdown Red Team, CCDC, CPTC

Anthony JeanPierre (**@ant**) - SecDev Member

# 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)  
Shreya Lakhkar (@shreya)  
Phil Fox (@xphilfox)

## UB SecDev Student Volunteer Staff

Rashid Abubeker (@riabubek)  
John Ryan (@jpryan2)  
Malav Vyas (@malavvyas)  
Edward Lynch (@edwardly)

\*Indicates a F21 lead instructor role

# Opening Remarks

Featuring Prof. Murray

# **UBNetDef Goals:**

Learn, Have Fun, Be Your Best

# Ground Rules

- Lectures: Recorded for archive (starting now!)
- Attendance: Taken weekly during lecture time.  
IT IS PART OF YOUR GRADE!!
- Homework: Weekly, deliverables due Thursdays  
7:04(:59) pm
- Late Policy: Everything submitted on time!
- COVID: Follow all guidelines put forward by the University and SUNY

# 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
  - 4.5. Field Trip: Data Center
  - 4.6. Assignment: Homework 1
    - 4.6.1. 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)

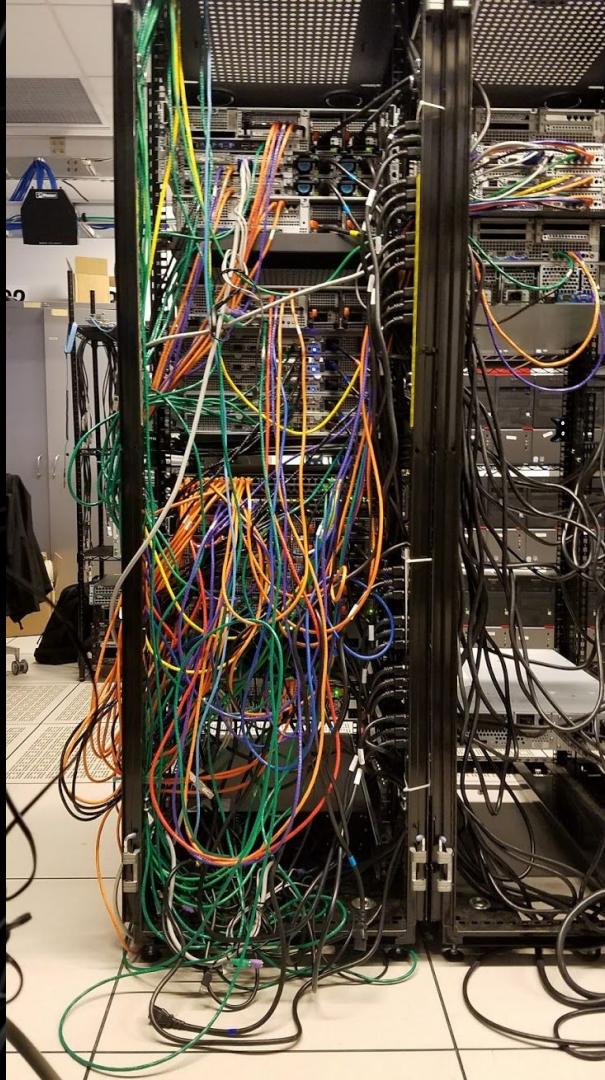
# Overview - UBNetDef

## Learners

The (for-credit!) courses

- SysSec: The gateway
- Network Security (NetSec)
  - Linux software and networking deep dive
  - Packet analysis
- Scripting Security (Phil 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...

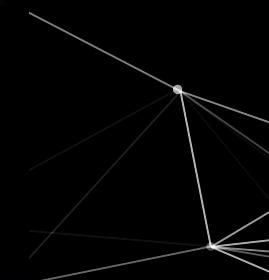
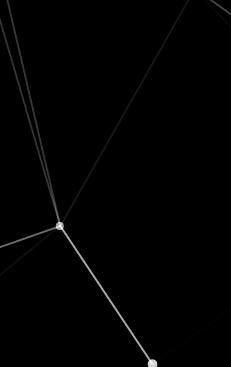


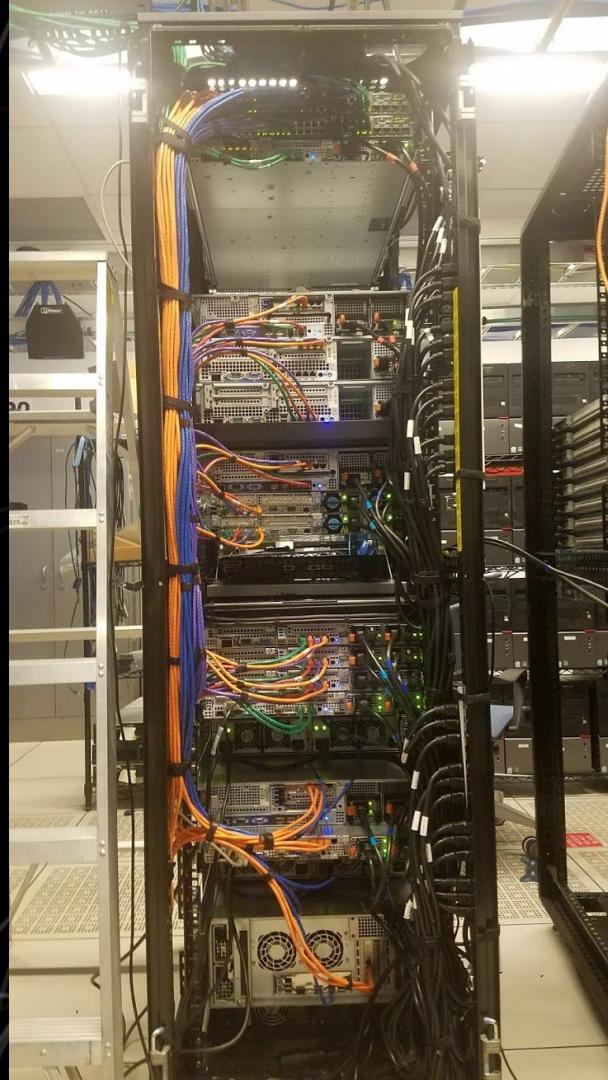


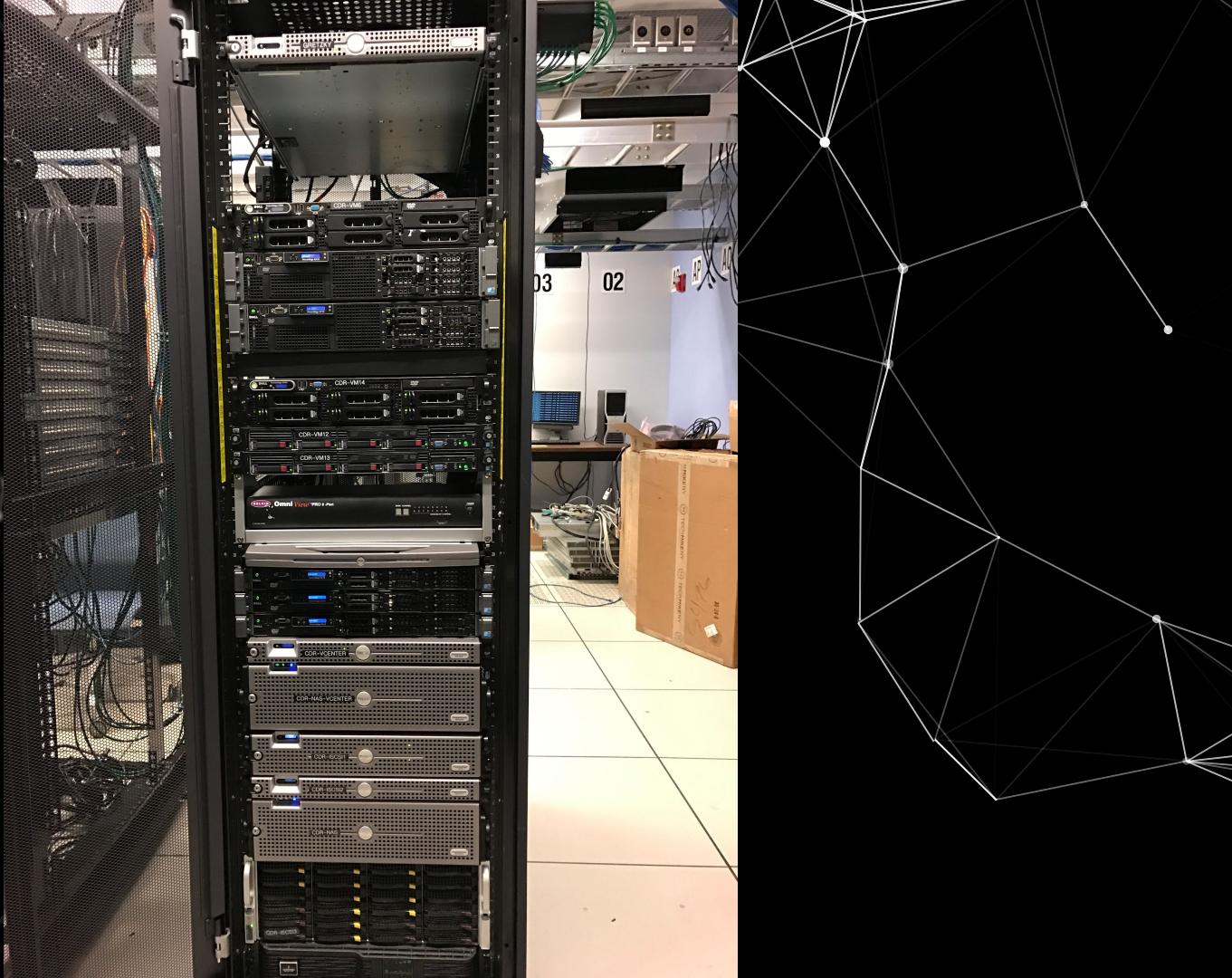
#WorkingTogether



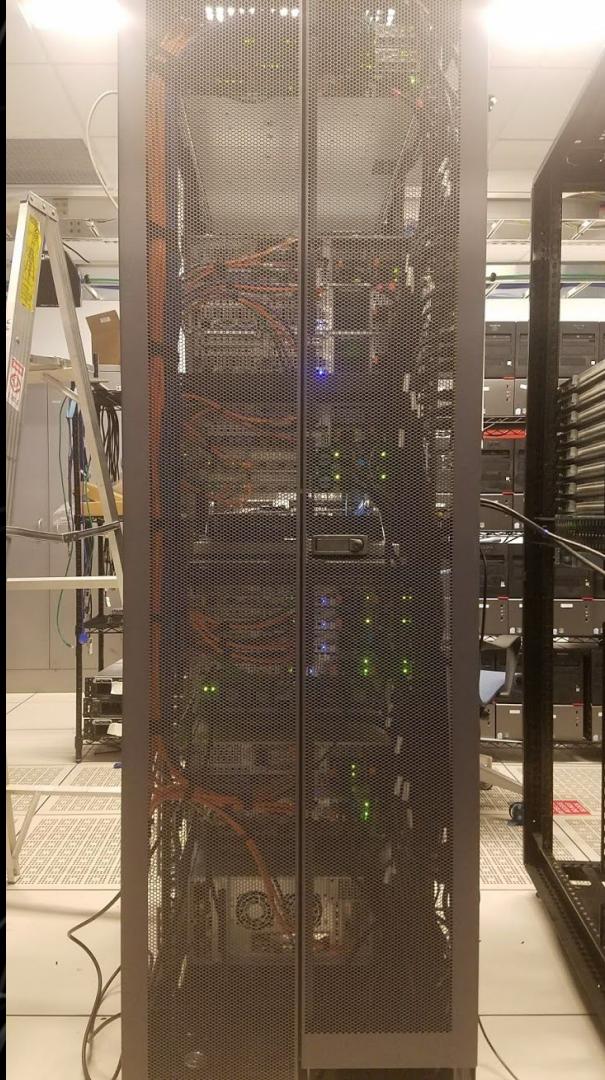








THE DOORS CAN CLOSE!!!



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”

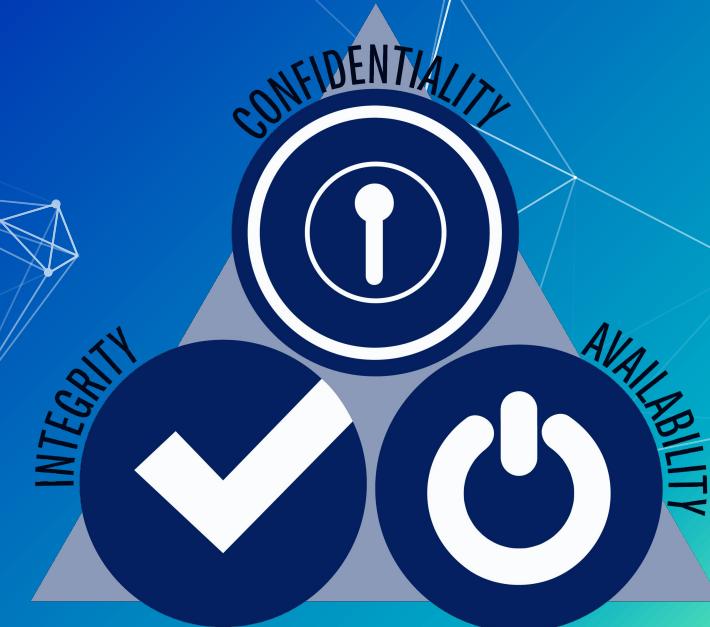


# Overview - Cybersecurity

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
  - 4.5. Field Trip: Data Center
  - 4.6. Assignment: Homework 1
    - 4.6.1. 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:

				
1000ft Solid Cat6a Blue Ethernet Cable, 10Gb, Spool <b>\$187.24</b> <a href="#">CableWholesale.c...</a>	Cat6 Riser Unshielded - Blue - 1000ft - Pull... <b>\$142.99</b> <a href="#">trueCABLE</a>  (21) Free shipping	Cat6 Shielded Solid PVC Network Cables - Blue - 100... <b>\$238.21</b> <a href="#">ShowMeCables</a>	Cat6A Riser Shielded - Blue - 1000ft <b>\$254.99</b> <a href="#">trueCABLE</a>  (11) Free shipping	1000ft Cat6 UTP 550Mhz Solid Cable 23awg Network... <b>\$59.99</b> <a href="#">Walmart - Dripstone</a>  (8) Free shipping

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

# An analogous scenario: Course materials

Additional clients (3):

The image shows a horizontal row of six laptop listings, each with a small thumbnail image, a brief description, and some purchase details. The laptops represent different clients or course materials.

- Recertified - Lenovo ThinkPad X Series X131e (628323U)...**  
\$99.99 refurbished  
[Newegg.com](#) - Ico...  
★★★★★ (141)  
Free shipping
- Recertified - DELL Laptop Latitude D630 Intel Core 2...**  
\$129.99 refurbish...  
[Newegg Business](#) ...  
★★★★★ (232)  
Free shipping
- Recertified - Lenovo/X240/Core i5-4200U...**  
\$235.99 refurbish...  
[Newegg.com](#)  
★★★★★ (250)  
Was \$303.99
- PRICE DROP CURBSIDE PICKUP**  
**Lenovo - IdeaPad 1 14" Laptop - AMD A6-Series - 4GB...**  
\$229.99  
[Best Buy](#)  
★★★★★ (4,403)
- HP 14 Series 14" Laptop AMD 3020e 4GB RAM 64GB...**  
\$269.99  
[Newegg.com](#) - ant...  
★★★★★ (10)  
Free shipping
- Recertified - Dell Latitude E5420 Laptop Intel i5 WiF...**  
\$209.00 refurbish...  
[Newegg.com](#) - CL...  
Free shipping

# An analogous scenario: Course materials

Windows 10 and Server licensing:

 <b>Windows Server 2019 STANDARD</b> Gold Microsoft Partner Microsoft Windows Server 2019 Standard - 16 Core... <b>\$529.99</b> Trusted Tech Team ★★★★★ (35) Free shipping	 <b>Windows Server 2019 Datacenter</b> PC-sales-online Free shipping	 <b>Windows Server 2019 16 Core Standard</b> Gold Microsoft Partner Microsoft Windows Server 2019 Standard 16 Core... <b>\$534.99</b> My Choice Software ★★★★★ (35) Free shipping	 <b>Windows Server 2016 STANDARD</b> Gold Microsoft Partner Windows Server 2016 Standard - 16 Core Download... <b>\$478.99</b> Trusted Tech Team ★★★★★ (550) Free shipping	 <b>Windows Server 2008 R2 Standard</b> Microsoft Windows Server 2008 R2 Standard - 16 CPU... <b>\$348.99</b> Softwarekeep USA ★★★★★ (67) Free shipping	 <b>Windows Server 2016 Standard 16 CPU</b> Windows Server 2016 Standard - 16 CPU - Download <b>\$258.00</b> PC-sales-online Free shipping	 <b>Windows Server 2019 Datacenter</b> Mic Server Datace <b>\$4,699</b> Neweg ★★★★★ Free sh
--	--	---	---	--	--	--

# An analogous scenario: Course materials

Webservers (3):

See Cisco Rack-mountable Computer Servers

Sponsored ⓘ

						
Cisco Multiparty Media 410v - rack-mountable - Xeon... \$17,647.99 CDW	Cisco Hyperflex System HX220c M5 - rack-mountable -... \$2,079.99 CDW	Cisco UCS SmartPlay Select C220 M5SX - rack-... \$14,029.99 CDW	Cisco UCS SmartPlay Select HX240c Hyperflex System -... \$20,989.99 CDW	Recertified - Cisco UCSC-C220-M3SBE= C220 M3... \$350.00 refurbish... Newegg.com - Net...	Cisco UCS C220 M4 High-Density Rack Server (Small Form Factor) \$11,491.99 CDW	Cisco UCS C220 M4 High-Density Rack Server (Small Form Factor) entry F... \$5,509 CDW
 (4)						

# 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.



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

# Virtualization: Let's look inside

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

# 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 UBLearn!
  - vCenter: <http://cdr-vcenter.cse.buffalo.edu/>
  - Use your full UB email for the login ID
- Check it out: You have a device!

# Breakout 02

Virtualization Activity

# Virtualization Activity

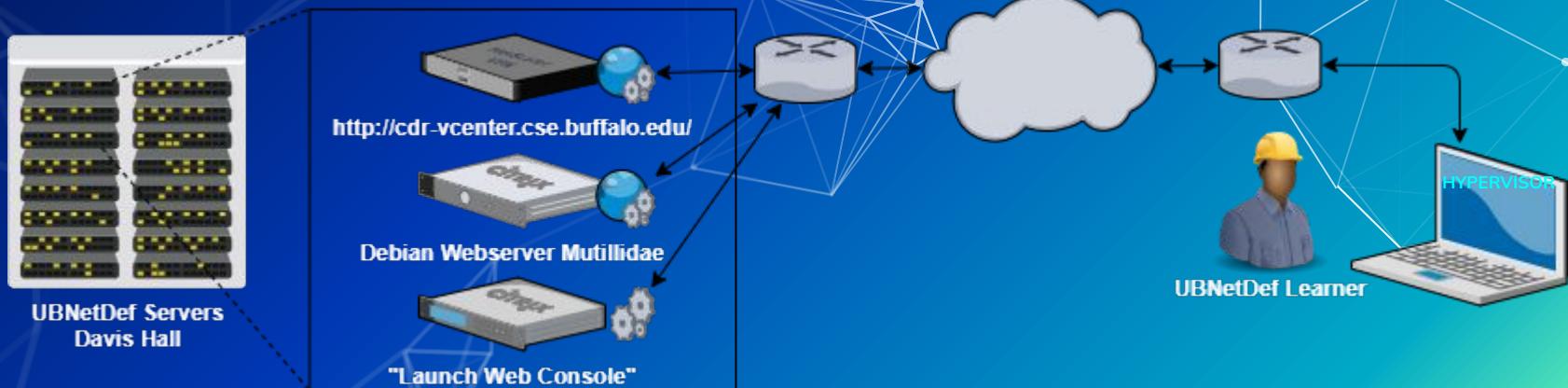
- Windows
  - Open your Windows VM
  - Try to use it. What do you observe?
  - And now, we will increase it to 8 GB of RAM
  - What do you observe?

# Virtualization Activity

- Linux
  - Open your Kali VMs
  - Start hashcat
    - hashcat -h
  - Try to crack the passwords in the first file!
    - hashcat -m 0 -a 0 -o cracked.txt targetedHashesEasy.txt /usr/share/wordlists/rockyou.txt
    - hashcat -m 0 -a 0 -o cracked1.txt targetHashes10.txt /usr/share/wordlists/rockyou.txt
  - Try to crack the passwords in the second file
  - What do you observe?

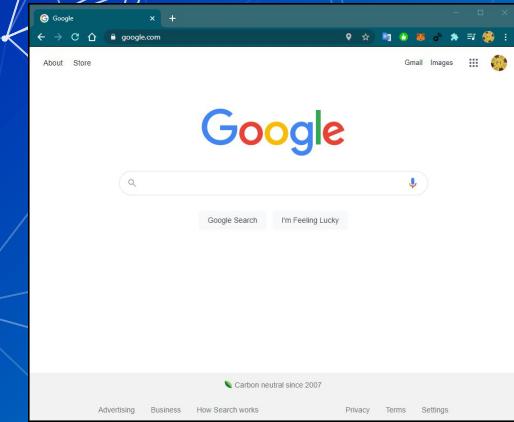
# Back to virtualization: How did we do that?

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



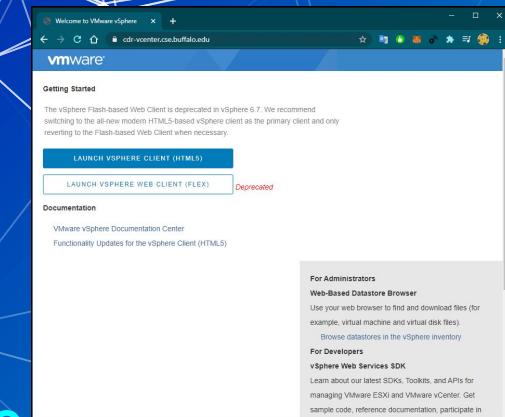
# Virtualization: What (you) the end user sees

- 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!



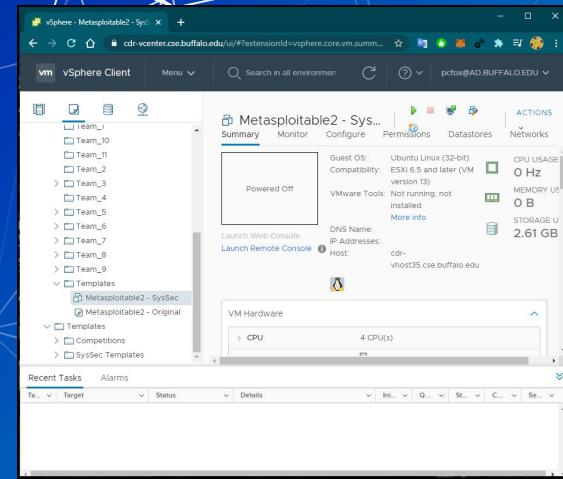
# Virtualization: What the end user sees

- 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!



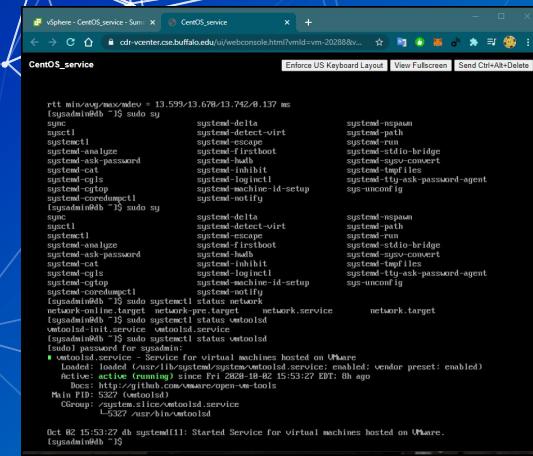
# Virtualization: What the end user sees

- 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!



```
rtt min/avg/max/wdev = 13.599/13.678/13.742/0.137 ms
[usudo@centos ~]$ systemctl status network.service
● network.service - Network Service
   Loaded: loaded (/usr/lib/systemd/system/network.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2020-10-02 15:53:27 EDT; 8h ago
     Docs: http://github.com/CanonicalLtd/network-tools
Main PID: 5327 (networkd)
   CGroup: /system.slice/network.service
           └─ 5327 /usr/bin/networkd

Oct 02 15:53:27 dh systemd[1]: Started Service for virtual machines hosted on VMware.
[usudo@centos ~]$
```

# **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
  - 4.5. Field Trip: Data Center
  - 4.6. Assignment: Homework 1
    - 4.6.1. **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
  - 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)
- 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 29<sup>th</sup>, 2020

# 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

## Contents

Executive Summary .....	2
Incident chronology .....	3
Relevant malware profiles .....	8
Recommended response .....	9
Means of remediation .....	9
Appendix A: Device address map .....	12
Appendix B: Table of observed significant events .....	13
Appendix C: Data integrity .....	14
Appendix D: Recovered malicious files .....	14
Appendix E: Analyst Cheat Sheet .....	14

# 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

```
[root@localhost ~]# /etc/sysconfig/network-scripts/ifcfg-ens192" 18L, 329C written
[usadmin@localhost ~]$ sudo systemctl restart NetworkManager
[usadmin@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 0.0.0.0 scope host
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens192: <BRD,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:56:86:50:17 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.10/24 brd 192.168.1.255 scope global noprefixroute ens192
            valid_lft forever preferred_lft forever
        inet6 fe80::26a3:5229:ec9b:4d scope link noprefixroute
            valid_lft forever preferred_lft forever

```

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.

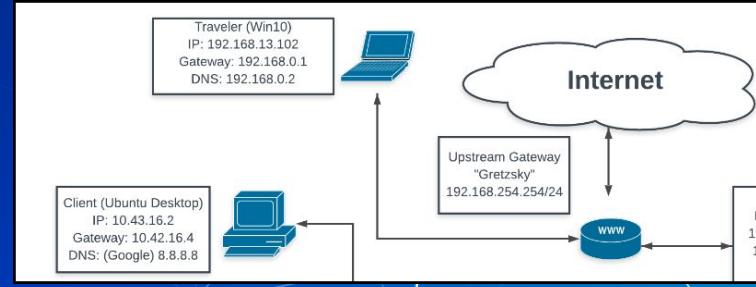
<sup>2</sup> Trend Micro, [REDACTED]

<sup>3</sup> ProofPoint Staff, [REDACTED]

November 28, 2020.

# 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: 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)

# Homework 1 (HW01)

- Posted to UBLearn 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!
- System state: Both client installations are complete and are network-connected.

# Launch a VM from .iso

- In vCenter:
  - Choose the less familiar operating system in the prior slide
  - Follow your mentor's instructions on how to launch an .iso!

# Breakout 03

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
  - 4.5. Field Trip: Data Center
  - 4.6. Assignment: Homework 1
    - 4.6.1. 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**
  - Launch a machine
  - Modify the virtual hardware settings
- We communicated the standards for **reporting**
- We described the homework process, this week's HW, and course resources

# Don't leave (yet)!

- Clarification on activities
- Homework help available
  - An early start gives you a huge edge on timely completion
  - Good time to address feedback for remediation when necessary

# Parting questions

Now is the time!

# Field Trip

Data Center

# Class dismissed

See you next week!