



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)

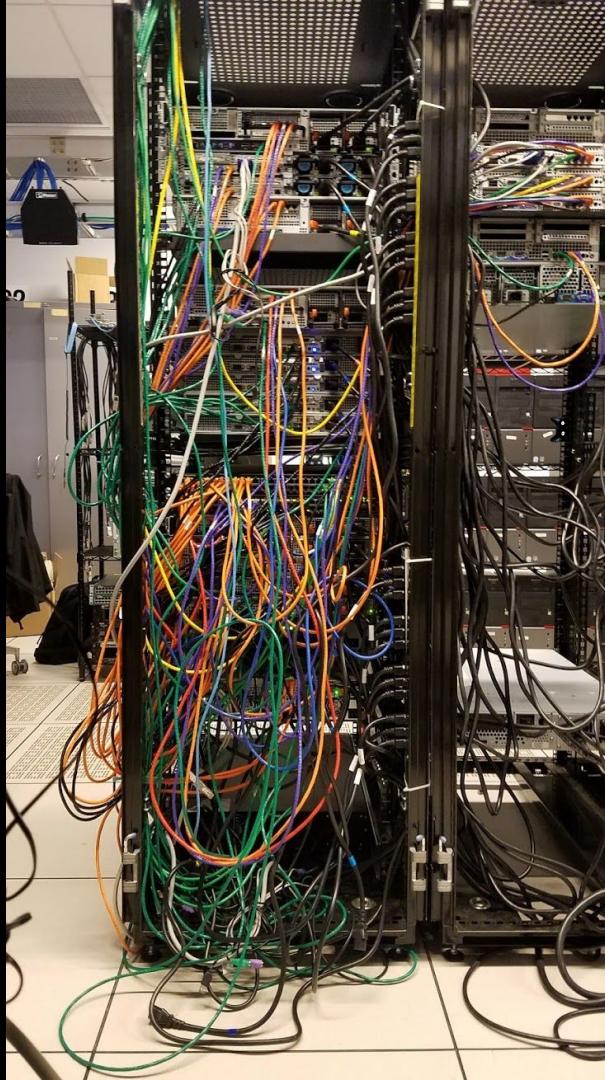
Overview - UBNetDef Learners

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



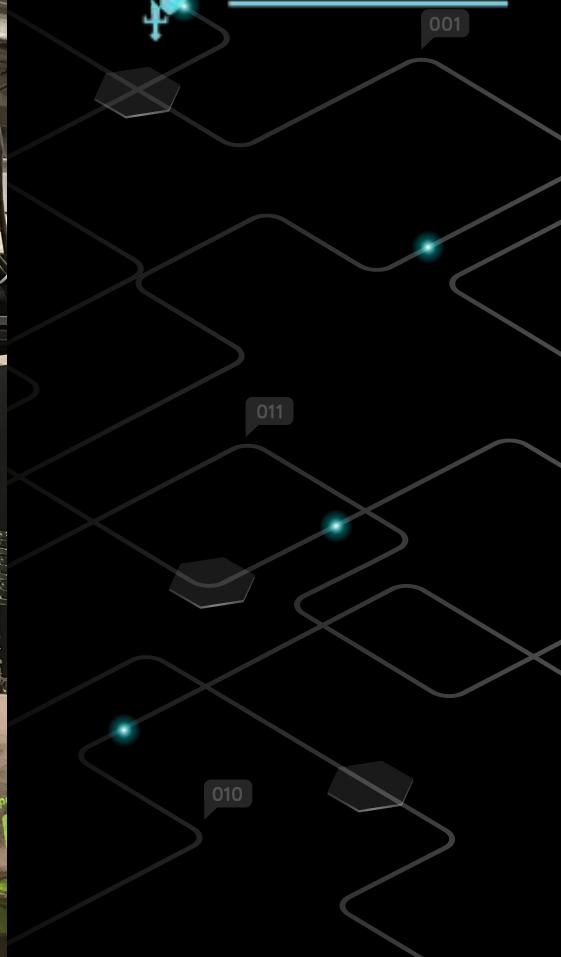
...only one

010

011

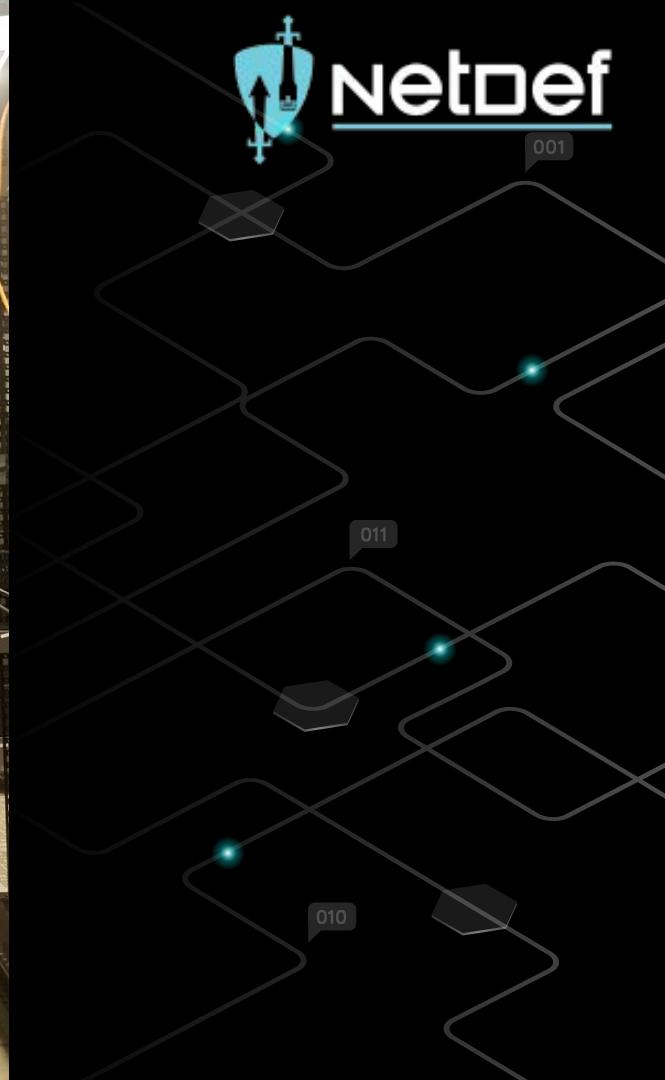
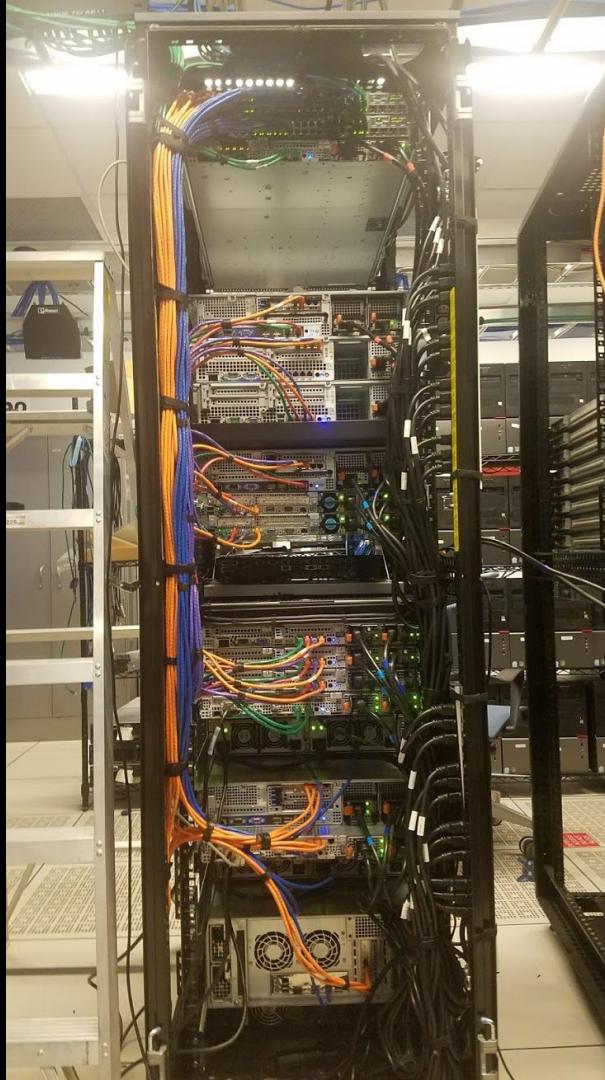
001

#WorkingTogether











001

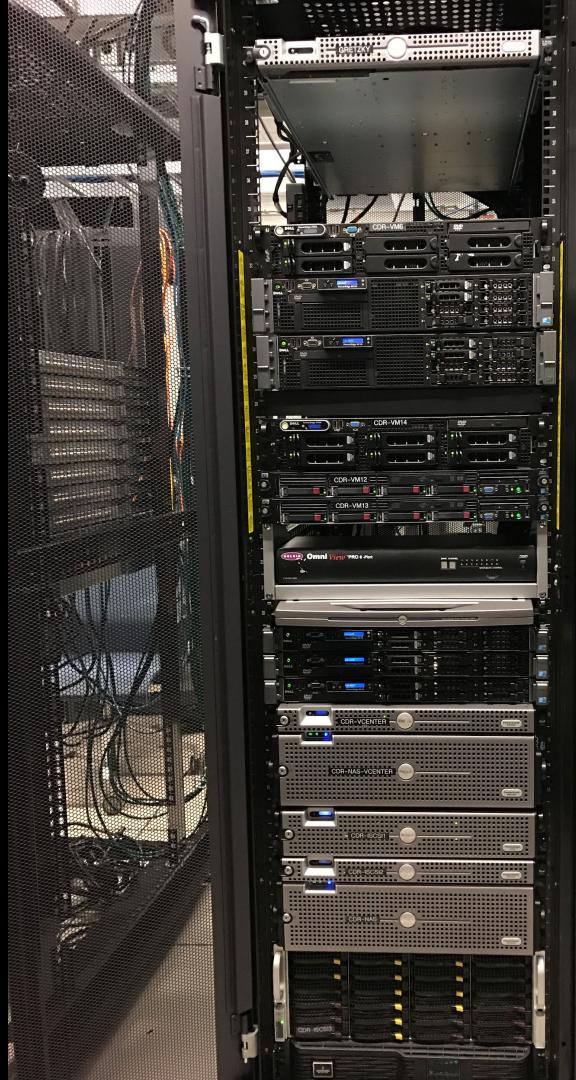
011

010

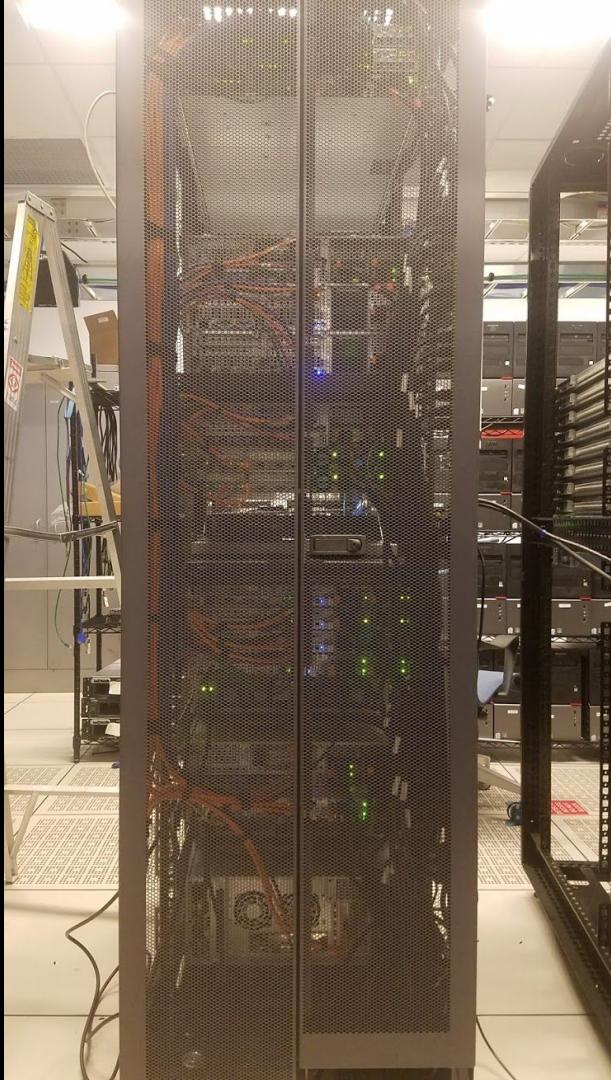


03

02



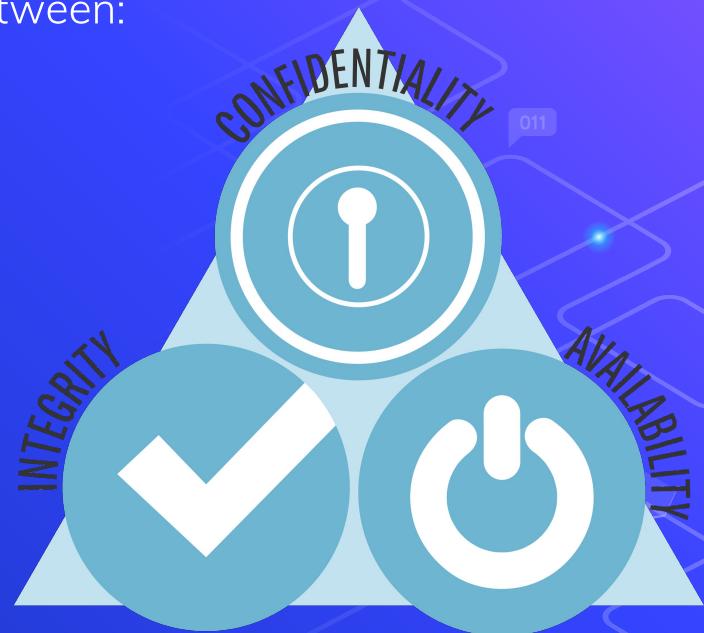
THE DOORS CAN CLOSE!!!



Overview - SysSec

What about this course?

- hexagon icon Investigating the boundaries and overlaps between:
 - pentagon icon Information Technology (IT)
 - pentagon icon Information Systems (IS) Management
 - pentagon icon Computer Hardware and Software
- hexagon icon ...through the lens of “cybersecurity”
 - pentagon icon Observe: The “cybersecurity triad”

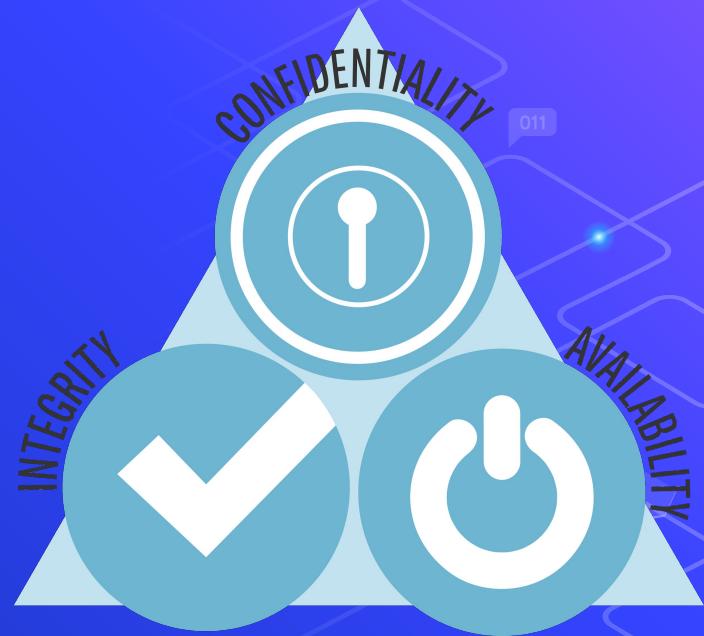


Overview - Cybersecurity

Discussion (roundtable):

What's the difference?

- Confidentiality
- Availability
- Integrity



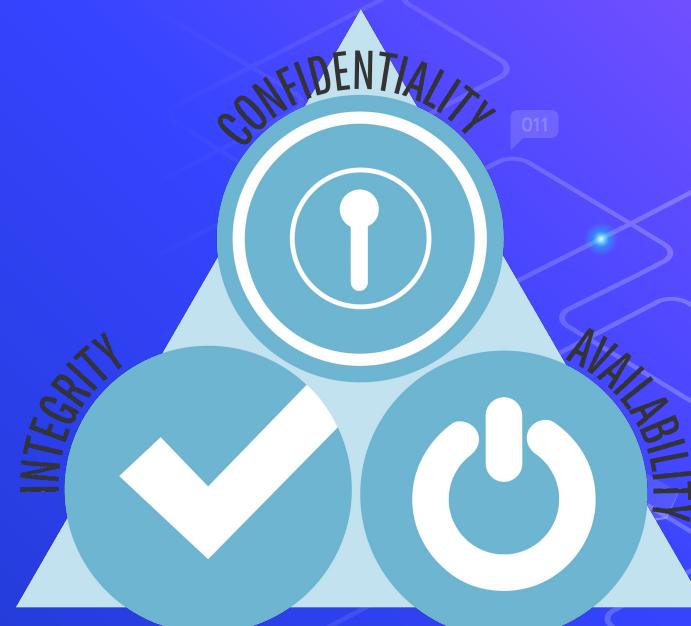
Overview - Cybersecurity

Discussion (roundtable):

What's the difference?

- Confidentiality
- Availability
- Integrity

Which is most important?



Overview - Cybersecurity

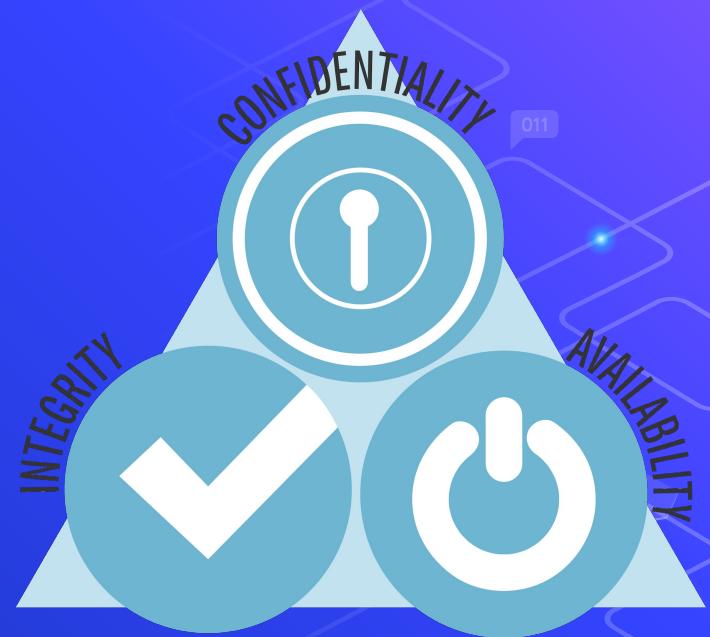
Discussion (roundtable):

What's the difference?

- Confidentiality
- Availability
- Integrity

Which is most important?

Can priorities between the three change?



Overview - Cybersecurity

Discussion (roundtable):

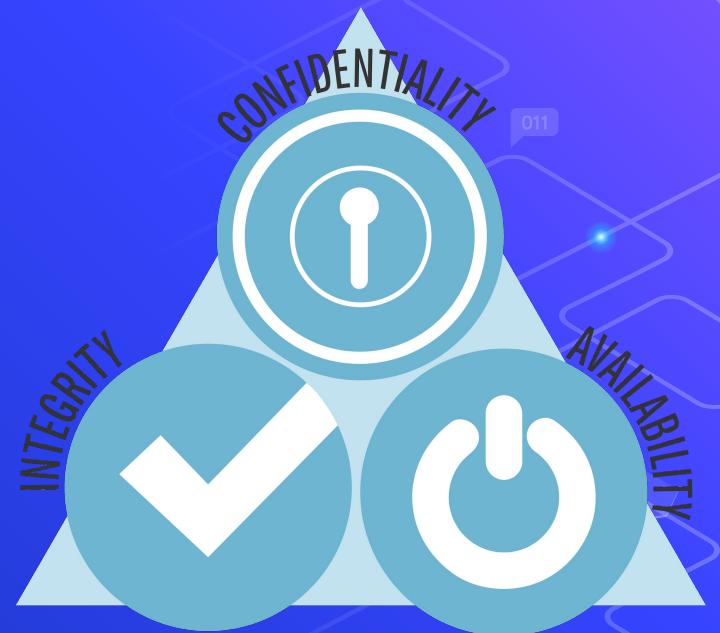
What's the difference?

- 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:

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

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

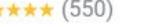
An analogous scenario: Course materials

Additional clients (3):

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

An analogous scenario: Course materials

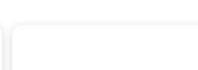
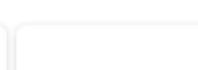
Windows 10 and Server licensing:

 Windows Server 2019 STANDARD  Microsoft Windows Server 2019 Standard - 16 Core... \$529.99 Trusted Tech Team  Free shipping	 Windows Server 2019 Datacenter PC-sales-online \$1,799.00 Free shipping	 Windows Server 2019 16 Core Standard  Microsoft Windows Server 2019 Standard 16 Core... \$534.99 My Choice Software  Free shipping	 Windows Server 2016 STANDARD  Windows Server 2016 Standard - 16 Core Download... \$478.99 Trusted Tech Team  Free shipping	 Windows Server 2008 R2 Standard  Microsoft Windows Server 2008 R2 Standard \$348.99 Softwarekeep USA  Free shipping	 Windows Server 2016 Standard - 16 CPU PC-sales-online \$258.00 Free shipping	 Windows Server 2019 Datacenter Newegg  Free sh
--	---	---	--	--	--	--



An analogous scenario: Course materials

Webservers (3):

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



(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/syssed/>
 - Also available on UBLearn!
 - ◊ 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/syssed/>
 - Also available on UBLearn!
 - ▷ 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/syssed/>
 - 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!

Virtualization: Let's look inside

- Login to vCenter
 - ◊ Primary course links available at <https://ubnetdef.org/courses/syssed/>
 - 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!
- 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:

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 1 (Arrogant) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Security Reset DB View Log View Captured Data

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite.

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

backtrack

Samurai Web Testing Framework

MySQL Toad HACKERS FOR CHARITY

Browser: Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
 PHP Version: 5.4.4
 The newest version of Mutillidae can be downloaded from SourceForge



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

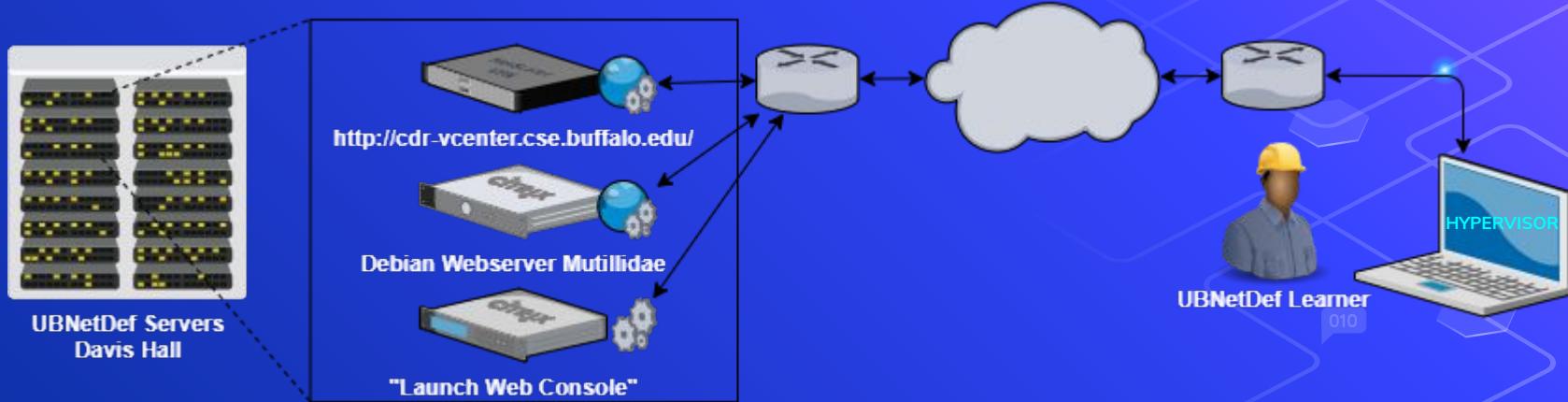
Incident Response

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?

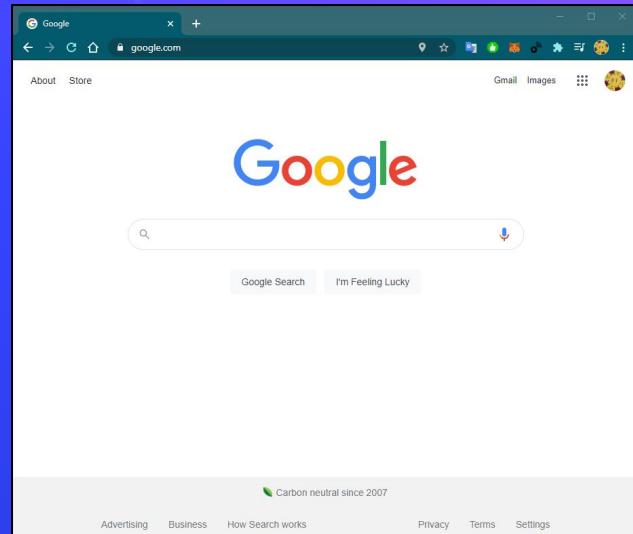
Back to virtualization: How did we do that?

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



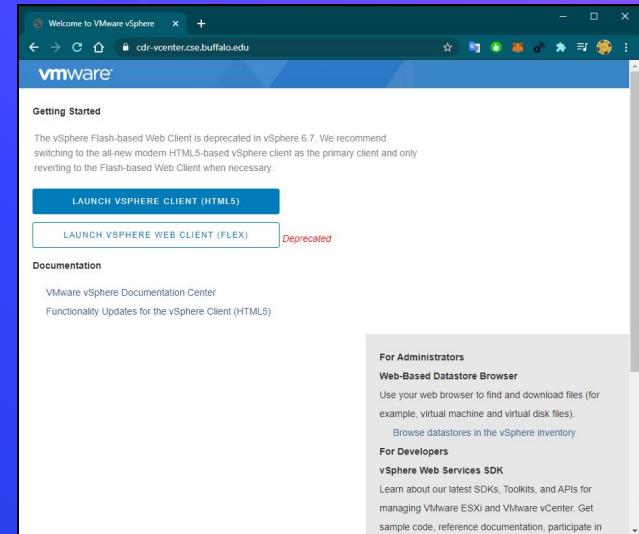
Virtualization: What (you) the end user sees

- 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!



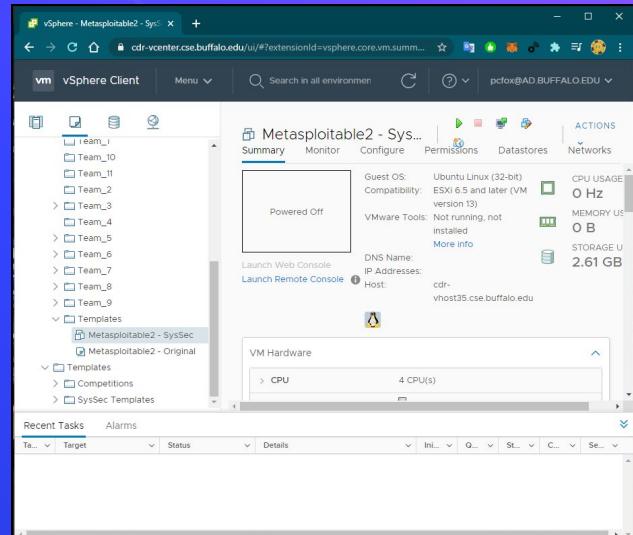
Virtualization: What the end user sees

- 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!



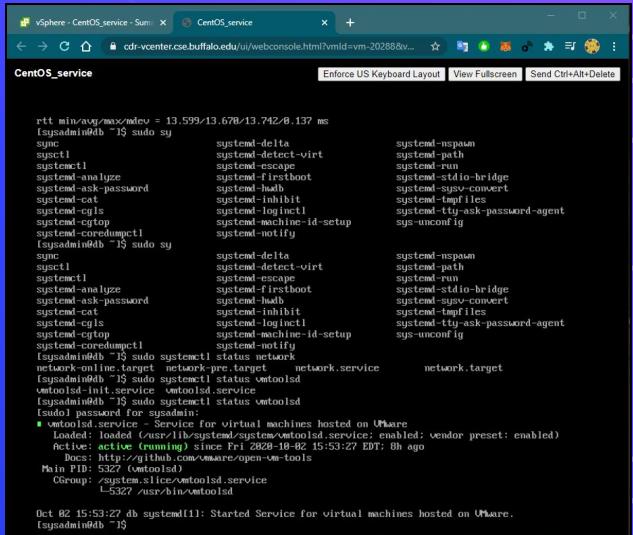
Virtualization: What the end user sees

- 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!



```

vSphere - CentOS_service - Summary | CentOS_service | + 
CentOS_service
Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete | 

rtt min/avg/max/jdev = 13.599/13.678/13.742/0.137 ns
[sysadmin@db ~]$ sudo systemctl status
● systemd-delta.service
● system-detect-virt.service
● systemd-escape.service
● system-firstboot.service
● systemd-journal-inhibit.service
● systemd-logind.service
● systemd-machine-id-setup.service
● systemd-notify.service
● systemd-path.service
● systemd-stdio-bridge.service
● systemd-sysv-convert.service
● systemd-timesyncd.service
● systemd-tty-ask-password-agent.service
● sys-configuration.service
● sys-fs-selinux.service
● sys-kernel-debug.service
● sys-kernel-hibernate.service
● sys-kernel-preempt.service
● sys-kernel-reboot.service
● sys-kernel-suspend.service
● sys-knfsd-remount-root.service
● sys-remount-rootfs.service
● sys-unconfig.service
● systemd-delta.service
● system-detect-virt.service
● systemd-escape.service
● system-firstboot.service
● systemd-journal-inhibit.service
● systemd-logind.service
● systemd-machine-id-setup.service
● systemd-notify.service
● systemd-path.service
● systemd-stdio-bridge.service
● systemd-sysv-convert.service
● systemd-timesyncd.service
● systemd-tty-ask-password-agent.service
● sys-configuration.service
● sys-fs-selinux.service
● sys-kernel-debug.service
● sys-kernel-hibernate.service
● sys-kernel-preempt.service
● sys-kernel-reboot.service
● sys-kernel-suspend.service
● sys-remount-rootfs.service
● sys-unconfig.service
[sysadmin@db ~]$ sudo systemctl status network
● network.service - Network interface configuration
  Loaded: loaded (/usr/lib/systemd/system/network.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2023-10-02 15:53:27 EDT; 8h ago
    Docs: http://github.com/vmware/open-vm-tools
  Main PID: 5327 (nettoolsd)
     Tasks: 1 (limit: 4915)
    CGroup: /system.slice/network.service
            └─ 5327 /usr/bin/nettoolsd

Oct 02 15:53:27 db systemd[1]: Started Service for virtual machines hosted on VMware.
[sysadmin@db ~]$ 

```



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 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!

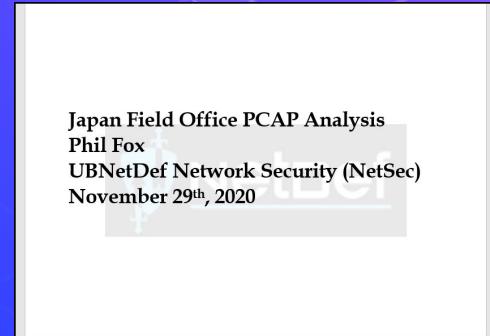
Coursework Support

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



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@centos ~]# /etc/sysconfig/network-scripts/ifcfg-ens192" 18L, 329C written
[tsusadmin@db ~]$ sudo systemctl restart NetworkManager
[tsusadmin@db ~]$ 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 lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host lo
        valid_lft forever preferred_lft forever
2: ens192: <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 10.43.16.1/24 brd 10.43.16.255 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::2563:5229%ens192 brd fe80::ff:fe%ens192 scope link nopref
        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.

² Trend Micro.

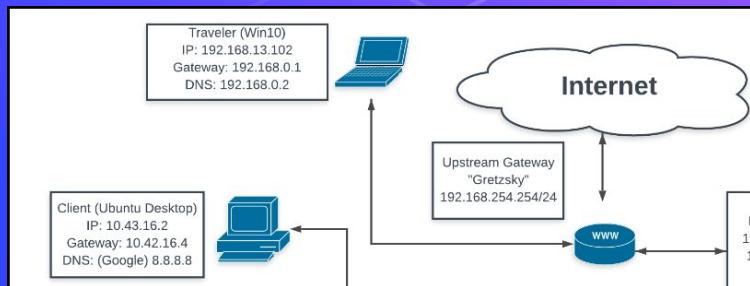
³ ProofPoint Staff

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 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!](#)
- [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

- hexagon In vCenter with your breakout room mentor:
 - triangle Choose the less familiar operating system in the prior slide
 - triangle One brave volunteer share your screen
 - triangle 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!