UB LOCKDOWN CYBERSECURITY COMPETITION

David J. Murray

Clinical Professor

djmurray@buffalo.edu

University at Buffalo
School of Management

Cybersecurity Outreach

UB GenCyber Camp

University at Buffalo School of Management

Cybersecurity Coursework - ubnetdef.org

about   courses   lectures   lockdown   wiki

Learn & Live Security
University at Buffalo Network Defense is a Cyber Security class & club

LEARN
Whether you're already a kali wiz or don't know what kali is, learn marketable skills in a growing field. Working in a collaborative environment, everyone is welcome and it's never too late to start.

BUILD
Use the concepts that you will learn to design, build, and secure your very own full-scale network. You will gain hands-on experience by applying the knowledge that you acquire.
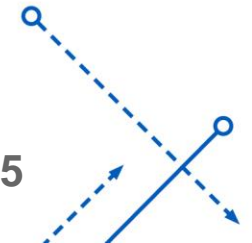
COMPETE
Step up and take your skills to the next level. Join a UBNetDef team and travel to competitions, where you can go head to head with top schools to compete for fame and prizes.
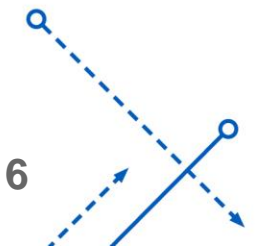
4

Cybersecurity Competitions

Agenda

- What is the UB Lockdown Cybersecurity Competition?

- Why should my students consider participating?

- How do we get involved?

- How should student teams prepare?

  - Google Classroom Materials

  - Open Cyber Arena Virtual Lab

UB Lockdown Background

- Lockdown HS v0, v1, v2 and v3 events since 2018

- 145 high school student participants

- Based upon collegiate Lockdown event

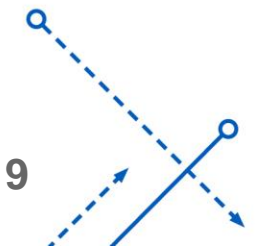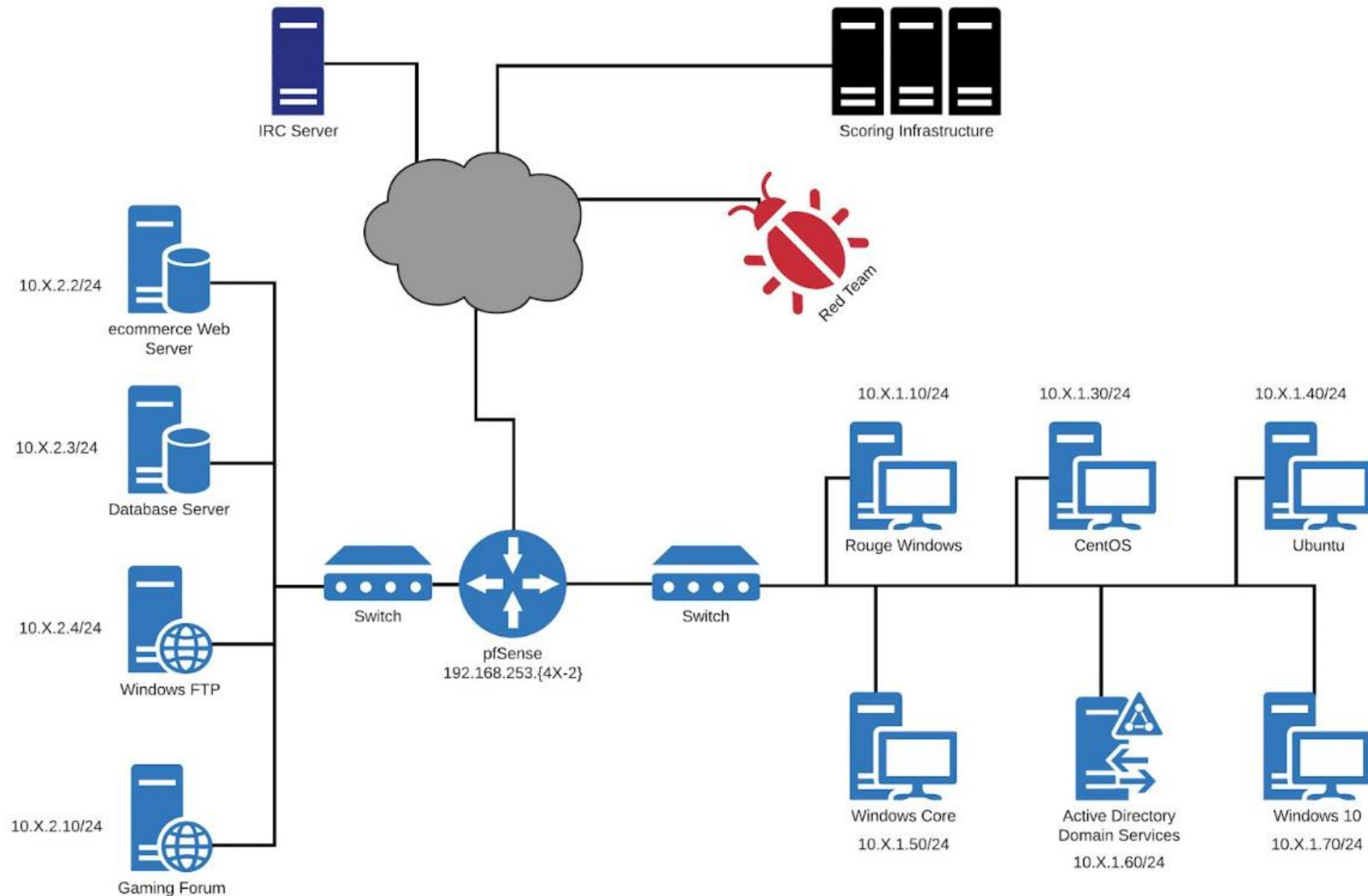|	
Amherst	**St. Mary's of Lancaster**
Buffalo Academy of the Sacred Heart	**Webster Schroeder**
Erie 1 BOCES Harkness	**Webster Thomas**
Lewiston Porter	**West Seneca Christian**
Mount St. Mary Academy	**Williamsville North**
Nardin Academy	**Williamsville South**
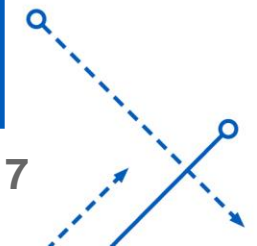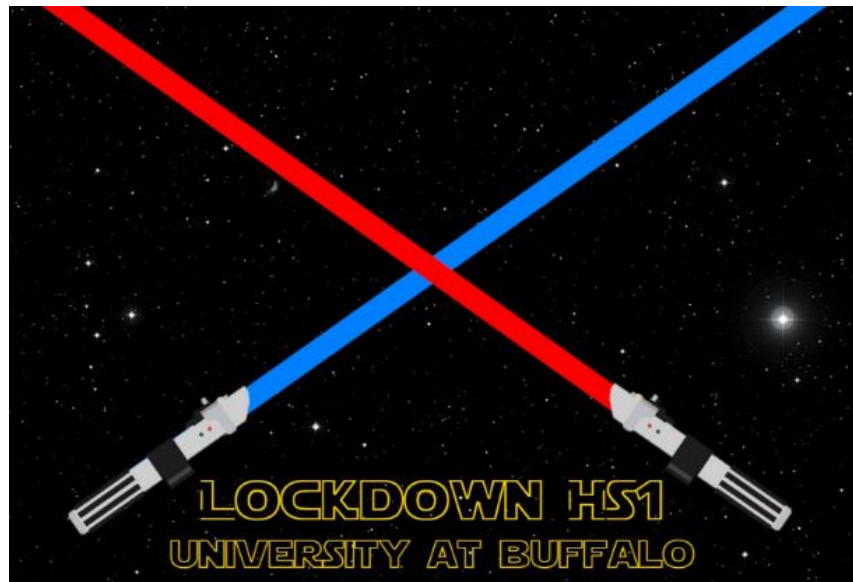
What is the UB Lockdown Cybersecurity Competition?

- Beginner level high school cyber defense competition
  - Red vs blue format, Cybersecurity CTF and other challenges
  - Guided and Applied tasks
  - Banking system
- Scoring based on:
  - Service uptime (50%) and tasks completed (50%)
  - Extra points earned with CTF and challenges

IRC Server

Scoring Infrastructure

Red Team

10.X.2.2/24
ecommerce Web Server

10.X.2.3/24
Database Server

10.X.2.4/24
Windows FTP

10.X.2.10/24
Gaming Forum

Switch

pfSense
192.168.253.{4X-2}

Switch

10.X.1.10/24
Rouge Windows

10.X.1.30/24
CentOS

10.X.1.40/24
Ubuntu

Windows Core
10.X.1.50/24

Active Directory
Domain Services
10.X.1.60/24

Windows 10
10.X.1.70/24

10

Round #223

Team	Rouge Windows	CentOS	Ubuntu	Windows Client A WinRM	Windows Core	AD DS	DNS	Magento	Database	FTP	Gaming Forum HTTP	Gaming Forum SSH
Team 1	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Team 2	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🔴	🔴	🟢	🟢	🔴
Team 3	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴
Team 4	🔴	🔴	🔴	🟢	🔴	🟢	🟢	🔴	🔴	🟢	🟢	🔴
Team 5	🔴	🔴	🟢	🔴	🔴	🟢	🟢	🔴	🔴	🟢	🟢	🔴
Team 6	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴
Team 7	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Team 8	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Team 9	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Team 10	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴

User Audit Guided Task

Wow, our company is growing at such a fast rate! I have no idea who is who anymore!! Hmm, maybe that's a bad thing. You know what? I want to know who is on what machine, so prepare a user audit (only need to report up to 3 users per machine) on the Linux CentOS Machine (10.X.1.30) and Windows Machine (10.X.1.70) in your network and document it in a professional manner. Please distinguish whether or not they are logged in as well. Please document this in a report that can easily be read. Once done with the report, show it to your consultant!

pfSense Firewall Guided Task

A new Windows malware has been reported to be infecting port 3333. We want you to block inbound TCP port 3333 using the pfSense router. To access the router's web interface, you are going to need to type the IP address of the router (pfSense) into your browser and log in through there. Show your consultant the new firewall rule blocking inbound TCP port 3333.

Purchasable Services

`$500: Irrelevant banker advice`

`$3,000: Direct Console access to any machine`

`$4,000: Snack time!!`

`$7,500: Consultant advice on a task`

`$13,500: Extra 15 minutes for a task`

`$15,000: Security Engineer (relevant) advice`

`$20,000: Submit one inject at any point you wish`

`$25,000: Red Team immunity for 15 minutes`

`$30,000: Revert machine back to a pre-competition`

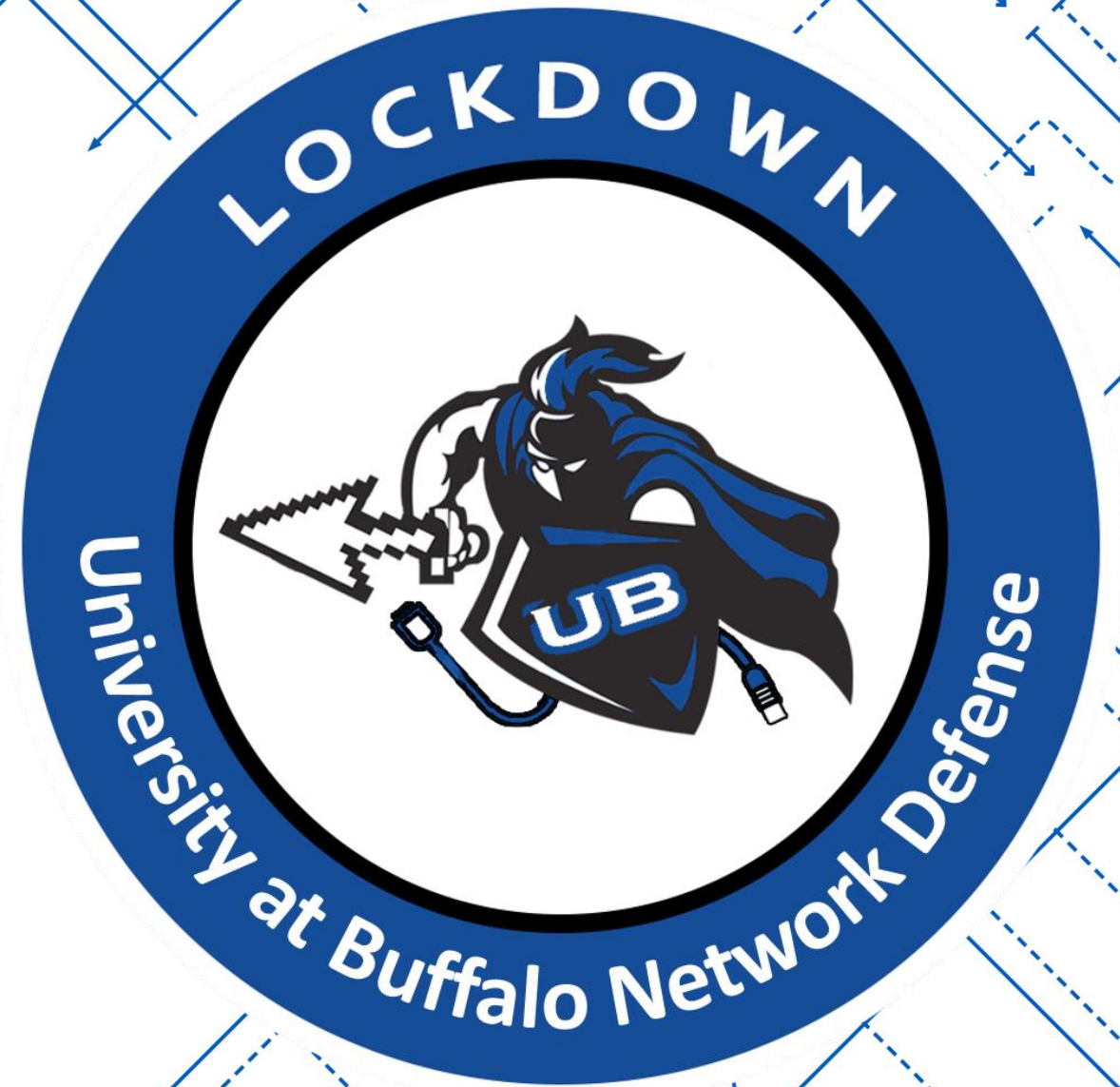# Why should my students consider participating?

- Emphasis on participant learning instead of competition

- Fun and unique hands-on challenge

- Interact with college student mentors and industry professionals

- Opportunity to work and compete as a team

- Exposure to collegiate style competitions

Google Classroom Materials

- 25 brief instructional videos and downloadable virtual machines

  - Windows

  - Linux

  - LAMP (Linux, Apache, MySQL and PHP)

- Enroll using a **personal** Google account and code **bgceeuh**

  - classroom.google.com

Open Cyber Arena Virtual Lab

- Ten hands-on cybersecurity/technology labs and videos

- Self-service virtual lab platform for teachers and students

  - Point and click setup of lab environment

  - Instructor access to account management, logs and student lab workspaces (pods)

- Shared workspaces to encourage collaboration and peer learning

- Runs on our 38 host VMware cluster - 825 GHz, 2.48 TB RAM

Open Cyber Arena Virtual Lab - arena.ubnetdef.org

- Introduction to Cyber Security and Networking

- Managing Services and the LAMP Stack

- Server Hardening

- Cryptography

- Packet Analysis

- The Operating System and an Introduction to Linux

- Advanced Networking Through Firewalls

- Identity and Access Management

- Vulnerability Assessment

- Digital Forensics

Open Cyber Arena Virtual Lab - arena.ubnetdef.org

Click "Lab resources" link to access lab content

UB LOCKDOWN CYBERSECURITY COMPETITION

David J. Murray

Clinical Professor

djmurray@buffalo.edu

lockdown.ubnetdef.org/highschool

arena.ubnetdef.org

University at Buffalo
UB | School of Management