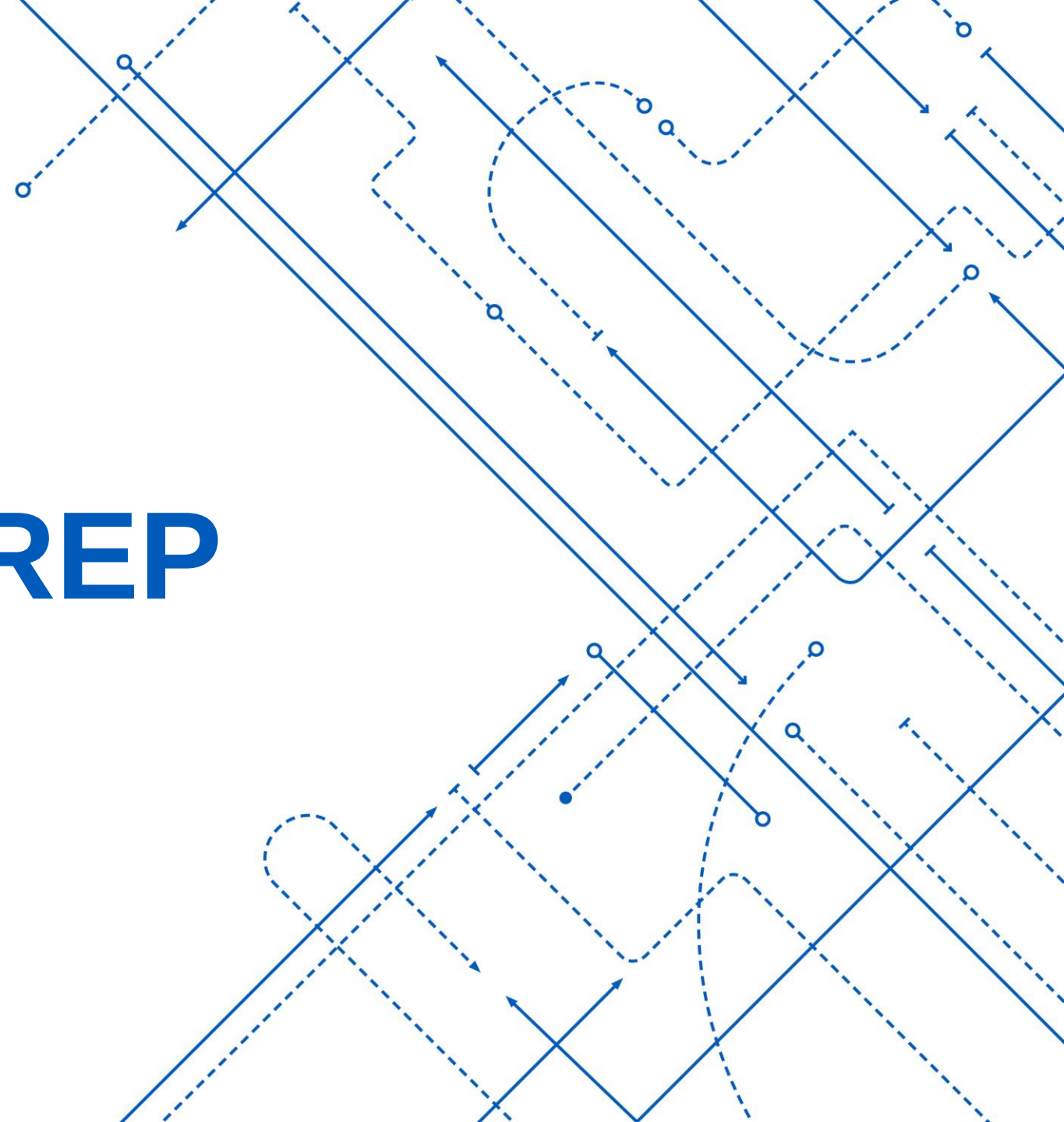
NECCDC QUALIFIER PREP

David J. Murray

Clinical Associate Professor

djmurray@buffalo.edu

University at Buffalo
School of Management



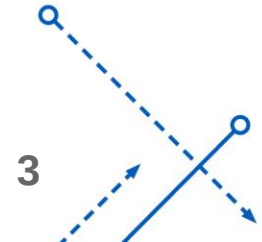
Acknowledgements

The contents of this presentation were compiled from feedback solicited from colleagues and former students. Kevin Cleary, James Droste, and Aaron Fiebelkorn were instrumental in sharing recommendations, lessons learned, and competition strategies. These ideas are freely shared with the goal of helping other competition teams maximize their NECCDC experience.

To further promote friendly competition, and a collegial atmosphere among the competitors of the Northeast Collegiate Cyber Defense Competition, you are also encouraged to share your lessons learned with the competition community.

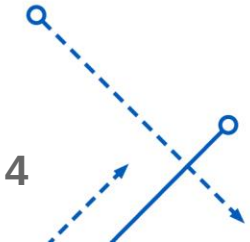
Disclaimer

This presentation should not be viewed as a “playbook” for winning cybersecurity competitions. Rather, it is a guide to help you maximize your overall experience and learning before, during and after a competition. Through research, learning and hours of practice, your team should develop a team strategy to be improved and built upon year after year.



Agenda

- UB Network Defense Overview
- UB Network Defense Goals
- Developing a Team
- Technical Preparation
- Competition Room Suggestions
- The First Ten Minutes
- Questions & Discussion

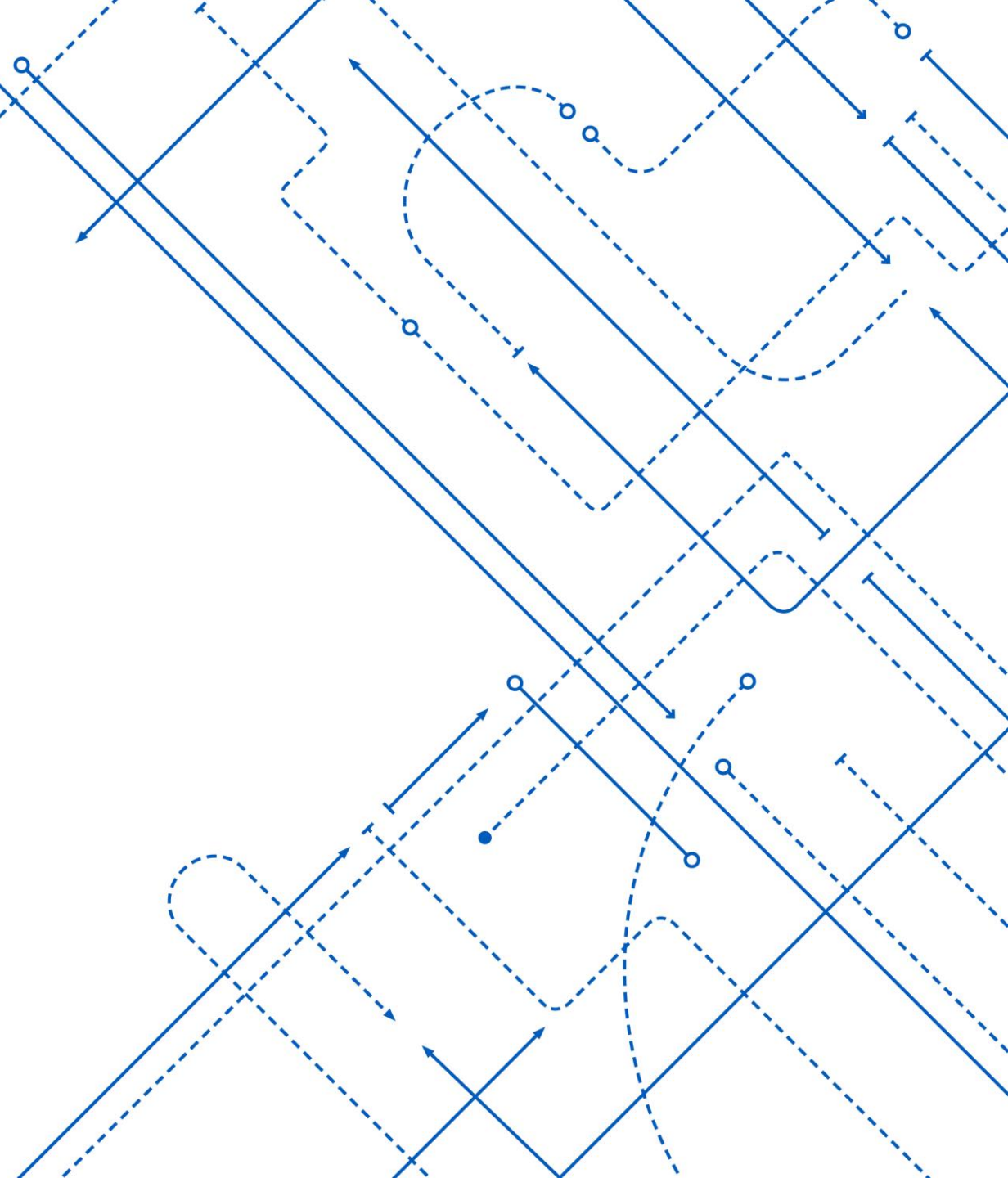


University at Buffalo
School of Management

UB NETWORK DEFENSE OVERVIEW

https://ubnetdef.org

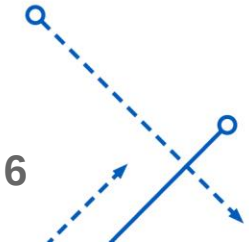
https://lockdown.ubnetdef.org



UB Network Defense Goals

- Learn
- Have Fun
- Don’t Give Up!

It’s not about winning, it’s about losing the least!

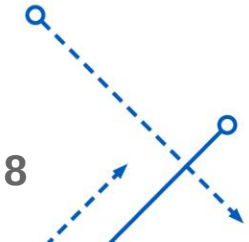


UB NECCDC Competitions - learn from our mistakes

- 2009 at RIT - 6th out of 6 teams - network down nearly all event
- 2012 at Northeastern - 10th - did not have networking expert
- 2013 at Maine - 10th - good team, but some bad luck
- 2014 at New Hampshire - Did not qualify; only 7 of 25 injects submitted
- 2015 at Syracuse - 10th - no network for Saturday/Sunday
- 2016 at Maine - 7th
- 2017 at RIT - 3rd

Developing a Team

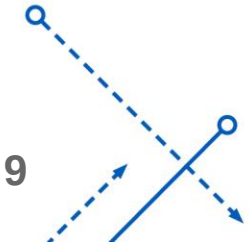
- Analogous to developing a sports team
- Carefully select motivated students with varied backgrounds and skillsets - Linux, Windows, Business, Networking, Project Management, Communication.
- Personalities matter
- Have a team bonding activity away from the work where they can build friendship and trust. If you don't have trust, you won't get anything done.
- Assign one person to handle the management of injects (taskmaster/timekeeper). Submissions should be professional!
- Determine system assignments prior to the competition
- Set expectations for team contributions and time commitment



Technical Preparation

- http://overthewire.org/wargames/
- https://www.nationalcyberleague.org/
- Network+ and Security+ resources
- https://lockdown.ubnetdef.org/

- Build and configure your own virtualized infrastructure.
- Services: DNS, AD, HTTP, HTTPS, SSH, MYSQL, Samba, email, FTP
- pfSense / Palo Alto / Cisco

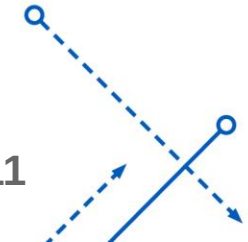


Baseline Linux Skills

- Comfortable using CLI and various distributions
- File system traversal
- File permissions
- Installing packages
- View/start/stop/restart services
- Netstat
- Monitor running processes
- Rudimentary log analysis
- User and Group Management

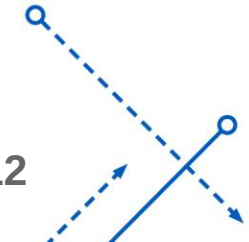
Baseline Windows Skills

- Manage Services
- Manage running programs in startup processes
- Process Monitor
- Event Viewer
- Rudimentary log analysis
- User and Group Management



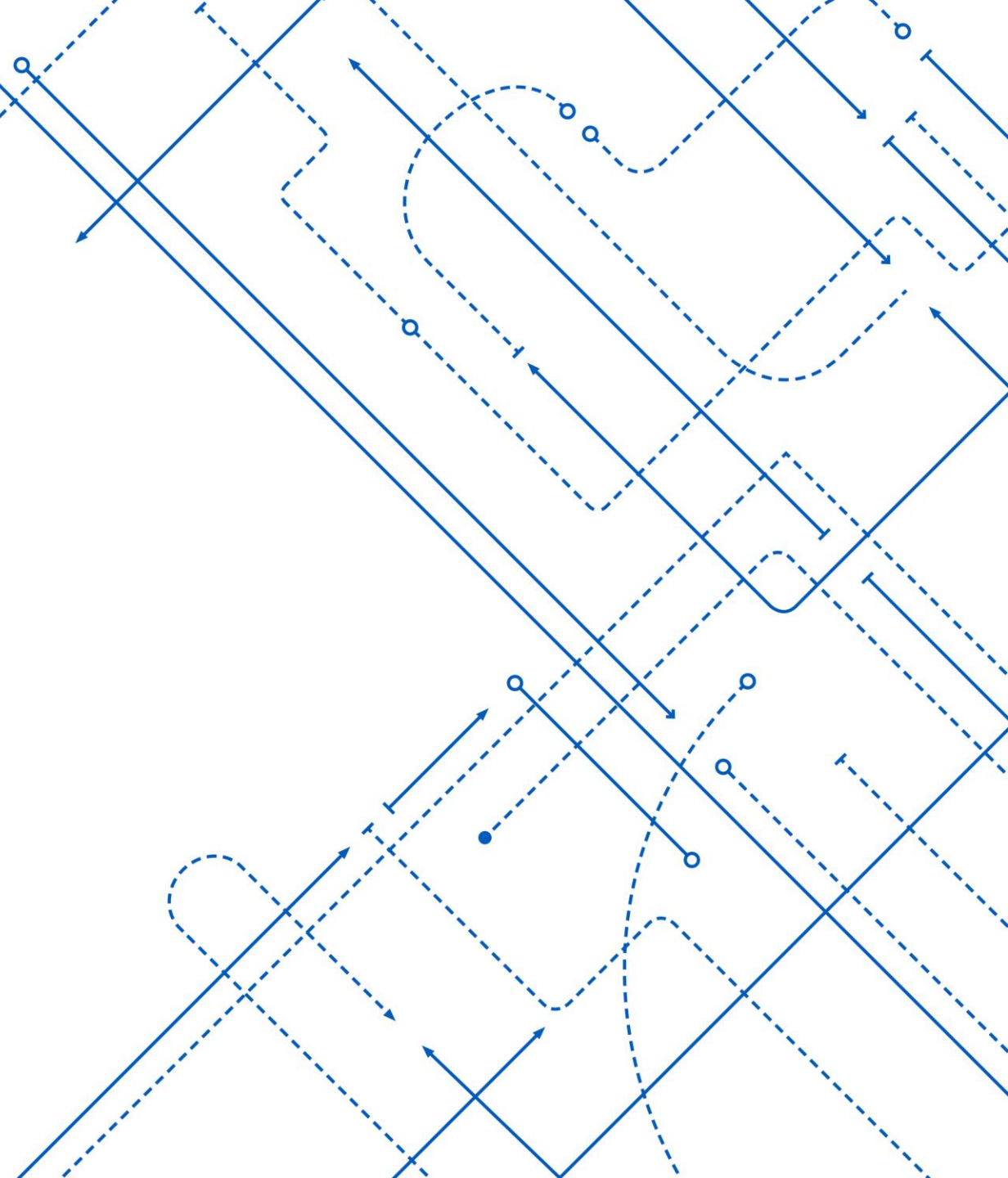
Baseline Networking Skills

- Manage router/firewall interfaces
- Create firewall rules
- Monitor traffic on spanning port
- Troubleshoot connectivity issues



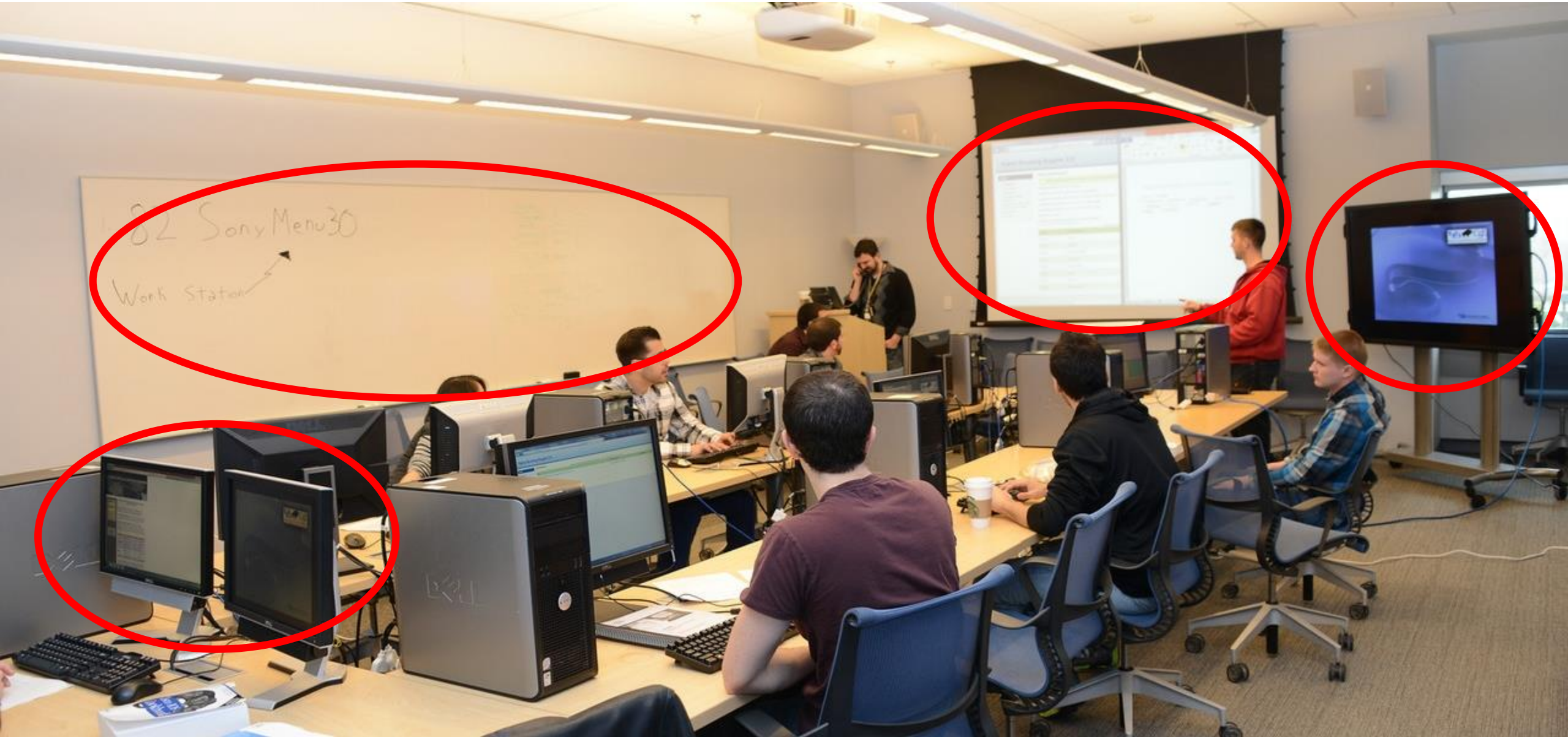
University at Buffalo
School of Management

COMPETITION ROOM PREPARATION



University at Buffalo
School of Management

University at Buffalo
School of Management

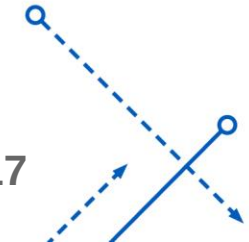


Competition Room Preparation

- Test connectivity to qualifier infrastructure **in advance**!
- Ensure adequate bandwidth and updated, compatible browsers
- Consider seating layout to facilitate team communication
- Drinks and snacks for competitors
- Whiteboard, markers and eraser
- Extra monitors
- Projector or screen

The First Ten Minutes

- Change default passwords quickly and **carefully**
- Scan network and build detailed topology on whiteboard (IP, running services, OS, etc.)
- Begin to lock down router/firewall
- Who is on your network? (users and accounts)
- Communicate, communicate, communicate
- Adjust assignments if necessary
- Begin to explore and understand systems (HTTP/MySQL dependency)
- Don’t shoot yourself in the foot! (forgot password, firewall rule issue, system misconfiguration, etc.)



University at Buffalo
School of Management

QUESTIONS & DISCUSSION