# Semester Startup Checklist

## BEFORE SEMESTER

### In General

- Make sure that current class lead, “seasoned” (1+ semester) SecDev members, and team leads for Lockdown are added to (`ubnetdef@buffalo.edu` aka `UBNETDEF-LIST@listserv.buffalo.edu`)
    - Send list to: Dave, Kevin, or James
- Add all of SecDev to the “SecDev” group in vCenter
    - Contact the nearest vCenter Administrator
- Get SecDev card access to B30
    - Send list to: Dave
- Define who will be responsible for updating the website. Add them as an *OWNER* in GitHub
    - Send list to: Nick, Jered, Stephen, Dave, or James
- If a SecDev member wants to contribute to the Wiki
    - Wiki accounts are now managed via FreeIPA (meaning that anyone getting an account on the Wiki would ideally have an account created on FreeIPA and given the appropriate group there)
    - Give them the groups “user” and “secdev” (may be named different on FreeIPA)
    - See your Free IPA Admins today for this
- Ensure all of SecDev is joined to the SecDev specific channel (`~secdev`)
    - You may want to consider clearing out old SecDev members, when a member graduates they should end up in `Leadership` if they still want to be apart of the class
- Ensure all of SecDev is joined to the SysSec channel (`~syssec`)

### Before First Class

- Create a schedule for the semester, look at the previous SysSec syllabus to see a topic-by-topic one
- Assign roles to each of the many weekly tasks
    - Clone VMs on vCenter
    - Set up attendance form
    - Lecture
    - Grade and update UBLearns
    - Post homework to homework.ubnetdef.org
    - Keep class docs in the Wiki updated
    - Upload lecture slides to website
- Upload the schedule to website
- Make homework.ubnetdef.org accounts for everyone, use default password and then have them all change it
- Discuss syllabus and agree to grading scheme, the current one as of System Security Spring 2019 works well
- Adjust syllabus with new SecDev members
- All SysSec should be emailed a few days before the first class with a link to the syllabus and with basic directions to the classroom

- [Typically before second class] Make vCenter accounts and folders for students + assign permissions

# DURING SEMESTER

## [Overview] Every Class "Checklist" of Tasks

- Who is going to lecture?
  - Make sure to give break every 50-60 minutes (This sort of depends on how tired the students are… but don't forget breaks, about 2 per class have worked great)
- Who will upload the lecture [PDF]?
  - Lectures are uploaded via `Git` to our website
- Who is going to quality check the assignment and reference with lecturer
  - Make sure it is clear on what the assignment goals are and parts are clear, responsible for updating confusing bits after the fact
- Who will make the homework.ubnetdef.org **Inject** and schedule it?
- Who will grade?
  - Grades are “owned” by one person, sheet is shared as needed and the grade “owner” will be responsible for uploading to UB Learns… FERPA…
  - You CAN grade directly on UB Learns, it might be even easier to do… Vince just hates UB Learns so he never did… and probably did it the hard way
- Who will make the attendance and make sure to work with lecturer on questions
  - Attendance form should have some key questions, some repetition of important material, some encouragement and some thanks for class
- Who “owns” the website, schedule updates, general updates, etc
- Who will make the VMs for the students
- Make sure everyone in SecDev helps in Mattermost!
- Make sure to have plans for items for all 3 hours, working sessions, lectures etc
  - If students are struggling feel free to review stuff
  - Highly recommend saving some time for required working sessions

**Make SURE to update the SecDev channel on Mattermost that you completed your task, this way everyone knows you did it!**

Each section below are what we consider our *core* classes, in each topic there is some information about reasoning and how we went about things. These are **NOT** playbooks and exact steps, but rather guidance on how we executed each topic and corresponding lecture.

# 1000 Mile Overview + Virtualization + Setup

## Disclaimer

- Typically this will *always* be the first class. If it's not the first class… wyd?
- Some students struggle to get to the rooms in the Jacobs center, so starting a few minutes late is OK
- For many students this is *completely* new, so keep reassuring the amount of help and guidance available

## Lecture Goals

- Make sure everyone knows what they will learn
- By the end of the class they should know if they want to be in Cybersecurity or not
- Why is NetDef different from any class they will take
- The Systems work they do here is a great foundation for entry level IT work
- Help Desk FTW!
- …

## Preparation

- All of the preparation is in the **Before First Section** bit above

## During Class

- This is class leads lecture, they should be speaking to the students in a confident manner
- Class lead starts the class off, makes sure all students are in the right place
- SecDev members introduce themselves, ice-breakers are fun
  - Makes a great example for the class when SecDev takes the ice-breaker seriously
- Students turn for the ice-breaker
- Overview of Syllabus, Website, Wiki, Homework Engine
- Have students sign the Code-of-Ethics, digital is ok - Ethics
  - Have them submit to `homework.ubnetdef.org`
- 10 minute break
- 1000 Mile Overview Lecture
- 10 minute break
- Virtualization and Infrastructure Overview/ Mini-Lecture

**During the first class you want to accomplish the items below, have a SecDev member send invites and the others make accounts if not done yet.**

- Invite all of SysSec and have get them in Mattermost
  - [After Registration] Force join (`/invite @username`) every SysSec student to the `~syssec` channel
- Have everyone connect into vCenter `cdr-vcenter1.cse.buffalo.edu`
- Have everyone sign-up on LucidChart
- Make everyone a `homework.ubnetdef.org` account and have them all sign and submit the `Code of Ethics`
- Anything that you don't get to above is homework for the students
  - You may not get to it all… don't worry about it we often don't

## Pitfalls

- This class MUST happen first, and you must get every student prepped by next class
  - This class should be treated as reserved and a must for the health of the rest of the semester
- Not having students read the syllabus before hand, make sure class lead emails them around Monday

    - Email should contain syllabus, location of class, time and what we will go over
- Do not forget one of the setup tasks, it will snowball the next few classes, (when Vince forgot to mention vCenter heh)

# Networking 101

## Disclaimer

- In the past we have taught this class as a general Networking foundation lecture, but found that was really to much for students. So we moved to a more focused lecture on our Infrastructure and what they will need to know for the labs and assignments. So a more targeted lecture on Networking so the students can be successful in the assignments without having to know everything.

## Lecture Goals

- Students to gain enough Networking knowledge to be successful in the assignments
- Gain a bit of understanding of the Networking around them (LAN, WAN, IP Addresses)

## Preparation

- Students *should* have folders in vCenter
- pfSense template should be cloned into those folders
- Point students to the Wiki where there will be documentation on “How to Load an ISO Image”
    - Please keep these doc's updated!
- Make sure there is enough static routes for all the students
- Upload the pfSense assignment to engine.ubnetdef.org
- Make sure everyone has signed the Ethics Policy **BEFORE** using vCenter
- Upload slides to website BEFORE lecture
- Make sure attendance is posted

## During Class

- Welcome the class back and start class off at 6:30pm
    - We want to set good precedence of class starting right away for students

        * House Keeping: is everyone in Mattermost, can log into vCenter, etc
- Networking 101 Lecture (60 mins)
- Break - 10 Mins
- Networking Lecture (30 - 45 mins)
- Topology Activity (20 - 30 mins)
- Break 10 Mins
- Explain homework's and how they can see them, recap of last week just different assignment
- Get everyone not caught up, caught up and have people work on installing pfSense
    - Point them to the Wiki for installing the ISO and have them read the assignment prompt
    - This is to help the students get used to Googling things and reading the doc's

- Keep them to 9pm, minimum

### Pitfalls

- Not teaching Networking to the infrastructure
- Networking in general...
- ...

## Windows

### Disclaimer

- Windows are NOT Just for Houses

### Lecture Goals

- Understand Client and Server relationships
- The internals of Windows and how the Operating System works
- How Active Directory works and is structured
- Domains
- How the client works when domain joined
- The power of group policy and mass identity management with Active Directory

### Preparation

- Post pfSense assignment playbook
- Two Windows virtual machines in each students folder
- Have previous assignment final grades in UBLearns
- Make sure the students know about Lockdown and get the registration form **OUT**
- Post Windows assignment typically given on Thursday and due *next* Sunday
- Reserve the last 45 minutes of class to help students progress on the assignment. Make sure everyone leaves making some progress

### During Class

- Greet class
- tell them if they have questions about setup of pfsense or wanna review it with a secdev memember to bring it up after class
- windows lecture
- break
- windows lecture
- start windows homework, make sure they know this is the longest assignment
    - make sure they know NOT to runbook the installs

### Pitfalls

- Not explaining *why* we need and *why* we use Active Directory

## Linux

### Disclaimer

- Many students think Linux is magic, our job is to fix that.
- Many don't understand shells and Terminals

### Lecture Goals

- Understand how the Linux Operating System works internally
- Gain understanding working with shells
- To gain confidence in controlling an Operating System through a shell and no GUI
- Learn some tools to use to troubleshoot networking

### Preparation

- Two virtual machines for a CLI box and GUI

### During Class

- Linux lecture
- Attendance
- Start having the students work on the Linux assignment.
    - Goal is to just install the Operating Systems and assign static ip addresses
    - They will use different boxes for the Services lecture, and use Linux box they setup here to interact with those new servers
- Make sure every students network is fully operational, catch people up who are behind

### Pitfalls

- None.

## Networking 102 (Typically Kevin)

### Disclaimer

- None

### Goals

- Kevin is the man

### Execution

- Make sure to upload Kevin's slides
- Verify every student understand they need to be attentive
- Make sure attendance is there

### Pitfalls

- None

## Services

### Disclaimer

- Students think Linux is magic, our job is to fix that.
- Many don't understand Shells and Terminals
- Many are not Software Developers, so they might find it difficult to understand shipping from code to software on a box

### Goals

- Understand what a *service* actually is
- Gain enough conceptual understanding to understand a LAMP stack
- Learn some Linux commands and tools to find and troubleshoot services
- Understand why services are so important - in the workplace and competitions

### Tasks Before Class

- Make sure there is two VMs for the Database and Webserver, these machines will go on the DMZ. Students can install a GUI on one and a CLI on the other.
- Upload the Lamp Stack assignment and make sure it is scheduled.
- Make sure attendance form is made.

### During Class

- Have class lead start class off at 6:30pm, sharp!
- How are assignments going? Does anyone need anything?
- Service Lecture
    - The services lecture in the past was around 80-90 mins, aim for the first part to be about 60 mins

- 10 Minute Break!
- Services Lecture (The last 20-30 mins)
- Attendance
- Start LAMP Assignment
    - SecDev member to show the students how to make the DMZ work, so we can avoid `pfctl -d`
    - If time, run through how to setup the database (You can either run through the install or make the VM for the students)

### Pitfalls

- TURN ON THE STUDENTS VM'S BEFORE CLASS SO WE DON'T BLOW UP VCENTER
- Make sure during the working sessions that SecDev is walking around and helping students
- Might be work it to use the laptops in the room instead of some students laptops
    - Especially Mac users... (Assuming we are still in vCenter < 6.0, this becomes nil after)

## Firewalls (Basic)

### Lecture Goals

- Gain an understanding of how Firewalls operate.
    - Inbound vs. Outbound.
    - Deny and Allow Rules.

### Preparation

### During Class

- Have class lead start class off at 6:30pm.
- Quick recap of last week and what we are going to do tonight. [10m]
- Firewall Lecture [1hr]
- Break [10m]
- Activity [30m]
- Homework working session [Until 9pm]

### Pitfalls

# Firewalls (Next Gen)

### Lecture Goals

- Placeholder

### Preparation

- Placeholder

### During Class

- Placeholder
- Placeholder

### Pitfalls

## MBA For a Day + Resume

## Risk Management