

Cyber Defense Organization

Fall 2018 Informational



Who?

You looked

We Are the Cyber Defense Organization

Sharing Practical Skills for Practical Situations. Our purpose is to help train students in the fundamentals of cybersecurity, and train for different competitions such as CCDC and other local events.



Workshops

Every week we hope to introduce a technical topic related to cybersecurity and have you work with it.



Competitions

The mission of the Collegiate Cyber Defense Competition (CCDC) system is to provide institutions with an information assurance or computer security curriculum a controlled, competitive environment to assess their student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems.



**NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION**

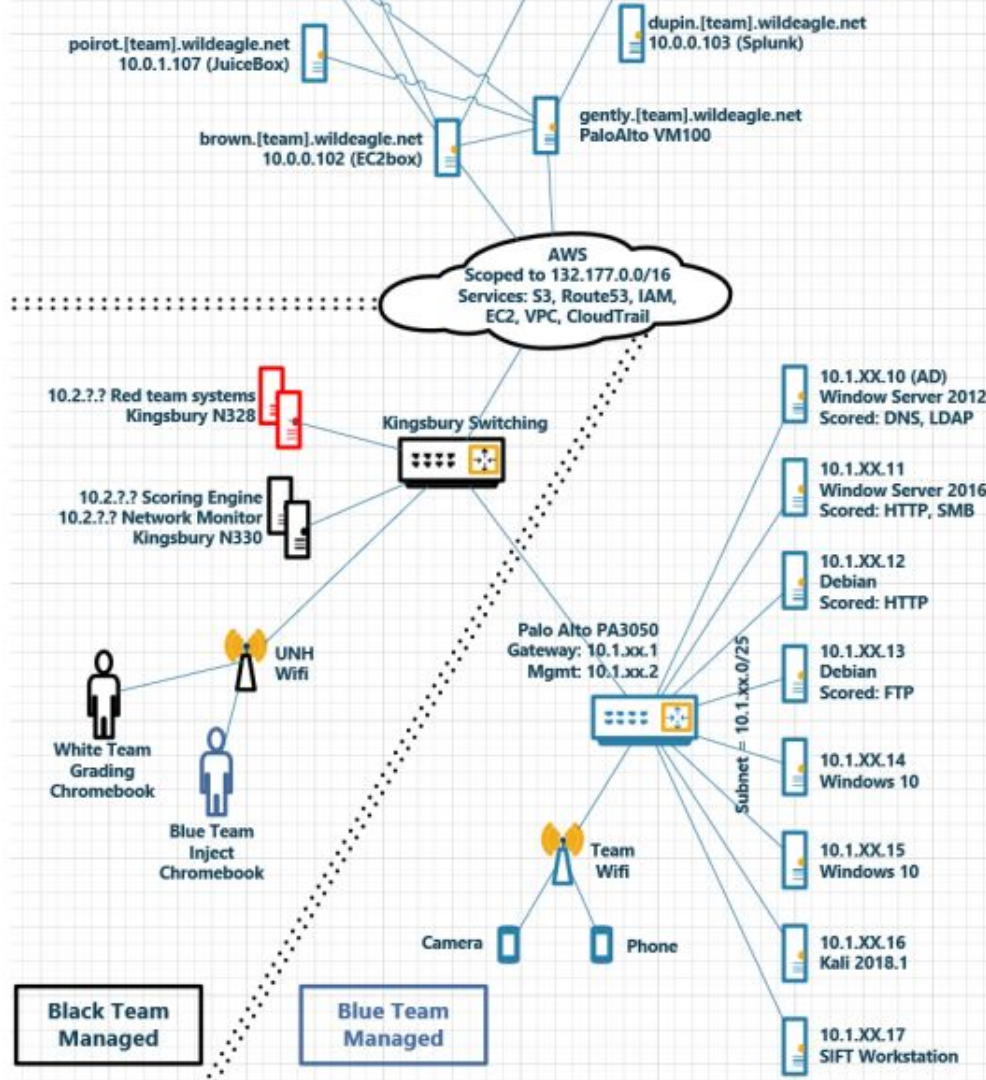
University at Buffalo Network Defense

Every semester we compete at a student run version of the competition run by a Buffalo.

Team A 1st Place

Team B 3rd Place





2018

National Collegiate Cyber Defense Competition
Presented By

Raytheon

Platinum Sponsors

UBER

Walmart
InfoSec



Program Sponsors



UNIVERSITY of WASHINGTON BOTHELL
CYBER SECURITY ENGINEERING

Gold Sponsors

information security

FireEye

BOEING

splunk

Silver Sponsors

FORCEPOINT

Sponsors

Carnegie Mellon University
Information Networking Institute

COMPTON STRIKE

G-C PARTNERS

IBM




Free Stuff that you can have! (Plus more)

There are a lot of free things you have
access to as a student!


Take advantage of them!

Online Training

- If you have an NYPL Library Card, you have **lynda.com**
- Free Cyber training - cybrary.it
- Quizlet
- Code Academy- codeacademy.com

Quizlet  CCNA


CCNA Flashcards
Browse 500 sets of CCNA flashcards


755 terms |  **ericmints5**

CCNA


Configure a Management VLAN Interface
(config)L#vlan VLAN NUMBER...
(config-vlan)#name NAME... (config-
vla...

Configure a sub-interface for Inter-
VLA...
(config)#interface INTERFACE.SUB-
INTERFACE... (config-subif)#no s...

90 terms |  **RachelAnnie_Harris**

CCNA 

Point to Point
Topology associated with WAN links

Ring
topology- associated with token ring
network and Fiber Distrib...


Networking - Juniper Networks

[Schedule of Classes](#)[On-Demand Courses](#)[Learning Paths](#)[All Courses](#)[JUNIPER ACADEMIC ALLIANCE - JNCIA JUNOS BOOT CAMP ON-DEMAND](#) [My History](#) | [My Profile](#) | [Log Out](#) | [Contact Us](#)[Learning Portal Home](#) > [Juniper Academic Alliance - JNCIA Junos Boot Camp On-Demand](#)[View By Topic](#) | [View By Date](#)

Juniper Academic Alliance - JNCIA Junos Boot Camp On-Demand



Juniper Academic Alliance - JNCIA Junos Boot Camp On-Demand

This is a one week on-demand course including narrated lectures and JNAA host provided labs that prepares Academic Alliance students to achieve the Juniper Networks Certified Internet Associate certification.

The JNAA JNCIA On-Demand content consists of following three items:

Networking Fundamentals eLearning Course: A 5-hour course that covers the fundamentals of TCP/IP networking.. This online, narrated, self-paced course walks students through the building blocks of networks including: how Ethernet Local Area Networks (LANs) operate; IP addressing and subnetting; and how data gets routed from one LAN to another using various Wide Area Networking (WAN) technologies..

Introduction to the Junos Operating System (IJOS) eLearning Modules: This 12-module ONLINE course, including 9 hands-on lab exercises, provides students with the foundational knowledge required to work with the Junos operating system and to configure Junos devices. The course provides a brief overview of the Junos device families and discusses the key architectural components of the software. Key topics include user interface options with a heavy focus on the command-line interface (CLI), configuration tasks typically associated with the initial setup of devices, interface configuration basics with configuration examples, secondary system configuration, and the basics of

Email Damira Pon, Moni Moni-Nwinia
mmnwinia@juniper.net

SIEMs

Splunk:

1. Training - https://www.splunk.com/en_us/training/free-courses/splunk-fundamentals-1
2. Product - Scale up to 500 MB data per day - https://www.splunk.com/en_us/software/pricing.html

SumoLogic

1. Training - <https://www.sumologic.com/online-training/>
2. Free Certs - <https://www.sumologic.com/learn/certifications/>
3. Premade environment - sumologic.com/wp-content/uploads/Labs-Using-Sumo-Security-Analytics.pdf

Cloud

1. AWS Cloud services

- a. Has a very generous Free tier - Need a credit/debit card

2. IBM Cloud

- a. Free plans is available
- b. Multiple free plans with modules
- c. Very fair
- d. Example:
 - i. NLP
 - ii. Chatbot
 - iii. Webpage services
 - iv. Etc.

3. Google Cloud Platform

- a. \$300 free when you first sign up.

Virtual Machines

- Oracle VirtualBox- [virtualbox.org](https://www.virtualbox.org)
- Uses .iso files to create a virtual environment that acts like a computer complete with its own operating system
- Great for experimenting with new operating systems and networks

Linux Open Source

All sorts of Linux Open source are here:

<https://www.linux.org/pages/download/>

Free Windows

You can get Windows Server and Client
Evaluation copies -

<https://www.microsoft.com/en-US/evalcenter/try>

Windows Server 2016

Evaluations | **180 days**

Project Server 2016

Evaluations | **180 days**

SharePoint Server 2016

Evaluations | **180 days**

System Center Configuration Manager
(version 1802)

Evaluations | **180 days**

Windows Server 2012 R2

Evaluations | **180 days**

Firewall



1. Interest in firewalls?

- a. Talk to Eric about details
- b. Free firewall to practice with PFSense

2. Other Firewalls

- a. Palo Alto - paid
- b. Windows Firewall
- c. Etc.
- d. Website list of free firewalls:
 - i. [More Firewalls](#)

Capture the Flag Sites

<https://www.hackthebox.eu/>

<https://www.vulnhub.com/>

<https://overthewire.org/wargames/>

<https://www.root-me.org/?lang=en>

Certification

Anything CompTIA is respected.

- Ask Tyler about the Security+
- Ask Liam about the CySA+
- Ask Eric or Anthony about Cisco Certifications (networking)
- Ask Michael about federal security clearance.

Networking Certifications/Training (Paid)

1. CCENT/CCNA (Cisco)

- a. HVCC offers courses
- b. Practice exams/test need to pay
- c. \$500+

2. CompTIA Network+

- a. Online website lists the exams
- b. Training provided in online form: Ebooks & Online tool Certmaster
- c. ~\$500

Forensic tool Certifications

1. ACE Certification

- a. Need a fully licensed FTK tool to take the test
- b. Free to take otherwise

2. EnCE Certification

- a. Used in our classes with a bit more training and studying you can be ready for the certification
- b. \$200 to pay for the certification

Build your own homelab

The software stack Liam uses -

<https://hackernoon.com/the-open-home-lab-stack-5e5858722fee>

Hardware - R710s are cheap right now. [Check ebay.](#)

Next Meeting - Intro To
Information Security.

Next Friday, 3pm, BB008.

Please join our myInvolvement
page! (It gets us a bigger budget.
And more cool stuff for you guys).

