CS53B: Firewalls and Threat Management
Foothill College Spring, 2018
Instructor: Timothy Ryan
Lecture Room: 4305, Wed 6:00PM – 9:50PM
Email: ryantimothy@fhda.edu
Office Hours: Tues 6:00PM – 7:30PM (Online and by appointment)
Website: https://foothillcollege.instructure.com or http://tinyurl.com/gofhda

Required Materials

Textbook: Zero Trust Networks, Building Secure Systems in Untrusted Networks
By Evan Gilman and Doug Barth (Authors). O'Reilly Media, Inc.

Course Description

Survey of topics in field of firewall, advanced threats and their characteristics. Students will learn how to manage Firewalls and advanced threats using security policies, profiles and signatures to protect networks against emerging threats.

Course Objectives

- Describe basic network security vulnerabilities.
- Explain firewalls and their features.
- Apply techniques used by firewalls to counteract vulnerabilities.
- Incorporate common solutions and strategies.
- Apply different Business Models and appropriate solutions.
- Describe firewalls use of digital signature authentication.
- Explain the operation of firewalls with Built-in Virus Scanning.
- Perform installation and configuration of Common Firewalls.

Student Learning Outcomes for CS 53A

- A successful student will be able to apply techniques used by firewalls to counteract vulnerabilities
- A successful student will be able to describe basic network security vulnerabilities

Foothill College Student Learning Outcomes:

https://foothill.edu/schedule/outlines.html

Opportunities and Resources

http://csopportunities.blogspot.com/
https://foothill.edu/stemcenter/

Evaluation

Course evaluation is based on the following:

Lab Activities	500 Points
Online Discussions	300 Points
Final Exam	200 Points

1000-900	= A
899-800	= B
799-700	= C
699-600	= D
599-Below	= F

Academic Honesty

Your instructor enforces the Foothill College Academic Honor Code. It is assumed that all students will pursue their studies with integrity and honesty. See course catalogue for details.

Lab Activities

Lab assignments will be completed using the online NetLab+ system which is available at the following URL: https://openlab.bayict.cabrillo.edu. Key features of each assignment will be discussed in class and emphasized with respect to course objectives.

Discussions

Each week will include an online Discussion. The Discussions will be completed within the Canvas Learning Management System and will be reviewed in class to provide background information and assist in preparing a thoughtful and articulate response.

Attendance

This class includes both an in-person and online section. The in-person section will be delivered within ConferZoom which allows active participation by all class members, it will also be recorded for later viewing.

Phones, Laptops and Classroom Etiquette

Use of cellular phones is prohibited during class time.

Special Assistance

To obtain disability-related accommodations, students must contact Disability Resource Center (DRC) as early as possible in the quarter. To contact DRC, you may:

- Visit DRC in Room 5400
- Email DRC at adaptivelearningdrc@foothill.edu
- Call DRC at 650-949-7017 to make an appointment

If you already have an accommodation notification from DRC, please contact me privately to discuss your needs.

Course Outline (Subject to Change)

Week	Date	Reading	Assignments
1	1/9	Chapter 1: Zero Trust Fundamentals	Lab #1: Initial Configuration *Online Discussion: Attack Progression
2	1/16	Chapter 2: Managing Trust	Lab #2: Interface Configuration *Online Discussion: Threat Models
3	1/23	Chapter 3: Network Agents	Lab #3: Security and NAT Policies *Online Discussion: Standardization
4	1/30	Chapter 4: Making Authorization Decisions	Lab #4: App ID *Online Discussion: Security Policy
5	2/6	Chapter 5: Trusting Devices	Lab #5: Content ID *Online Discussion: Trusted Platform
6	2/13	Chapter 6: Trusting Users	Lab #6: URL Filtering *Online Discussion: Single Sign-On
7	2/20	Chapter 7: Trusting Applications	Lab #7: Decryption *Online Discussion: Code Review
8	2/27	Chapter 8: Trusting the Traffic	Lab #8: Wildfire Lab #9: User ID *Online Discussion: Encryption
9	3/6	Chapter 9: Realizing a Zero Trust Network	Lab #10: Global Protection *Online Discussion: BeyondCorp
10	3/13	Chapter 10: The Adversarial View	Lab #11: Site-Site VPN Lab #12: Monitoring and Reporting *Online Discussion: APTs
11	3/20	Verizon Data Breach Report	Lab #13: Active/Passive HA *Online Discussion: Review (Not Graded)
12	3/27	Final Exam	

***Hybrid Course Information**

This course includes two "hybrid" hours per week. These "hybrid" hours are conducted within the Canvas Learning Management System (LMS) and not in a face-to-face class session on campus. In order to fulfill the participation requirements for these "hybrid" hours, students are expected to read the appropriate material and complete the Online Discussion as indicated above each week. Student participation during the "hybrid" hours is mandatory.