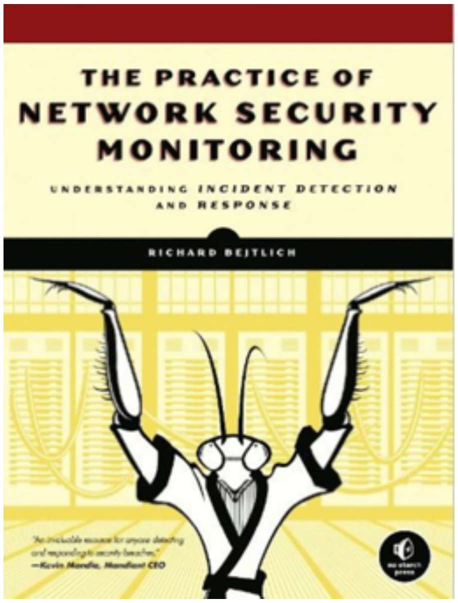
THE PRACTICE OF
NETWORK SECURITY
MONITORING
UNDERSTANDING INCIDENT DETECTION AND RESPONSE
RICHARD BEJTLICH
"An invaluable resource for anyone detecting and responding to security breaches."
—Kevin Mandia, Mandiant CEO
no starch press

CNIT 50: Network Security Monitoring

Fall 2017 Sam Bowne

`77816 Tue 06:10-09:00PM MUB 388`

Catalog Description

Learn modern, powerful techniques to inspect and analyze network traffic, so you can quickly detect abuse and attacks and respond to them. This class covers the configuration and use of Security Onion, a popular open-source Linux distribution designed for network security monitoring.

Advisory: CNIT 106 and 120, or comparable understanding of networking and security concepts.

Course Justification

Firewalls and antivirus are not enough to protect modern computer networks--abuse and attacks are common and cannot be prevented. Instead, networks are now monitored to detect security incidents, and security teams respond to them to limit the harm they cause. This class prepares students for jobs in monitoring and incident response, providing skills that are in high demand.

This course is part of the Advanced Cybersecurity Certificate.

Student Learning Outcomes

Upon successful completion of this course, the student will be able to:

A. **Explain the importance of network security monitoring and compare it to other types of defenses, such as firewalls**
B. **Implement and configure Security Onion to detect abuse and attacks on networks**
C. **Detect intrusions on the server-side and client-side of networks, and respond effectively to limit the damage they cause**

Textbook

"The Practice of Network Security Monitoring: Understanding Incident Detection and Response" by Richard Bejtlich, No Starch Press; 1 edition (July 26, 2013), ASIN: B00E5REN34 Buy from Amazon

Quizzes

The quizzes are multiple-choice, online, and open-book. However, you may not ask other people to help you during the quizzes. You will need to study the textbook chapter before the lecture covering it, and take the quiz before that class. Each quiz is available for one week, up till 8:30 am Saturday. Each quiz has 5 questions, you have ten minutes to take it, and you can make two attempts. If you take the quiz twice, the higher score counts.

To take quizzes, first claim your RAM ID and then log in to Canvas here:

https://ccsf.instructure.com

Live Streaming

Live stream at: ccsf.edu/webcasts

Classes will also be recorded and published on YouTube for later viewing.

Schedule

Date	Due	Topic
Tue 8-29		1: Network Security Monitoring Rationale
Tue 9-19	Proj 1 due Quizzes Ch 1 and Ch 2-3 due before class	2. Collecting Network Traffic: Access, Storage, and Management 3. Standalone NSM Deployment and Installation
Tue 10-10	Proj 2 & 3 due Quiz Ch 4-5 due before class	4. Distributed Deployment 5. SO Platform Housekeeping
Tue 10-31	Proj 4 & 5 due Quiz Ch 6 due before class	6. Command Line Packet Analysis Tools
Tue 11-21	Proj 6 due Quiz Ch 7 & 8 due before class All extra credit due	7. Graphical Packet Analysis Tools 8. NSM Console
Tue 12-12	Proj 7 due All extra credit due	Last Class: TBA
Tue 12-19		Final Exam (Optional)