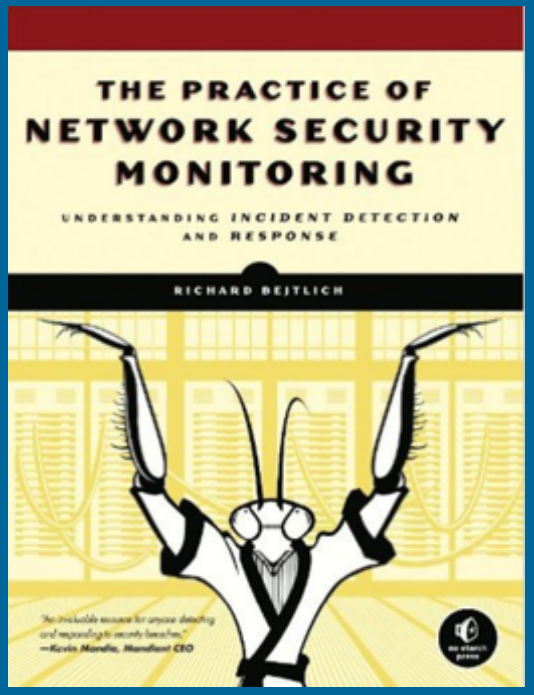
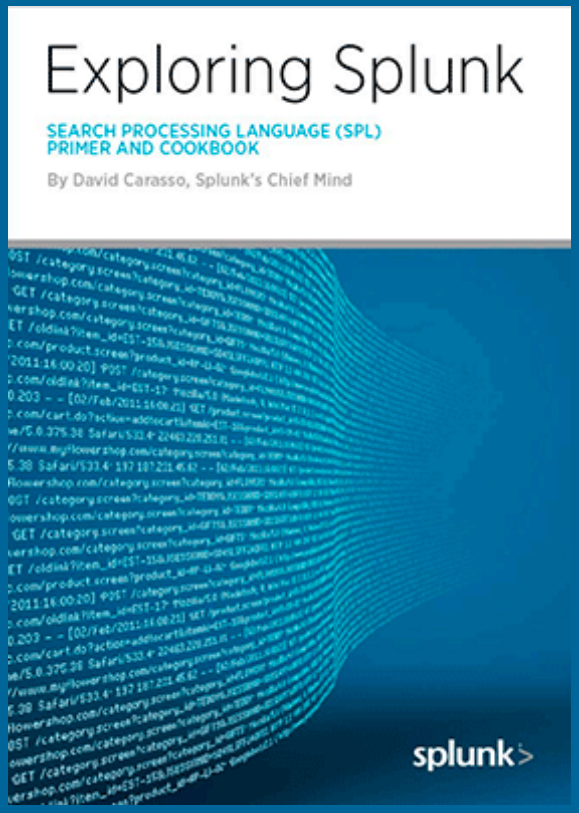
CNIT 50: Network Security Monitoring

Fall 2017 Sam Bowne





Scores

77816 Tue 06:10-09:00PM *Moved to MUB 388*

Schedule · Lecture Notes · Projects · Links · Home Page

Catalog Description

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

https://ccsf.instructure.com

Live Streaming

Live stream at: ccsf.edu/webcasts

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

Live Streaming for Kahoots

During the Kahoots, I'll also stream the class via Zoom.

Join from PC, Mac, Linux, iOS or Android: https://zoom.us/j/4108472927
Meeting ID: 410-847-2927

Schedule

Date	Due	Topic
Tue 8-29		1: Network Security Monitoring Rationale

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Tue 9-19	**Proj 1 due** **Quizzes Ch 1 and Ch 2-3 ***	**2. Collecting Network Traffic: Access, Storage, and Management** **3. Standalone NSM Deployment and Installation**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Tue 10-10	**Proj 2 & 3 due** **Quiz Ch 6 ***	**6. Command Line Packet Analysis Tools**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Tue 10-31	**Proj 4 & 5 due** **Quiz Ch 7 & 8 ***	**7. Graphical Packet Analysis Tools** **8. NSM Console**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Tue 11-21 **Proj 6 due** **9. NSM Operations**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Tue 12-12	Proj 7 due All extra credit due Quiz Quiz Ch 9 * & due There will be no Quiz on Ch 10 or 11	Last Class: No Lecture Security Apprenticeship Talk at 6:30 in MUB 140 Open lab in S214 after that event

---

Fri 12-15 - Thu 12-21	Final Exam available online throughout the week. You can only take it once.

---

* Quizzes due 30 min. before class

Lectures

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Policy · Schedule

Part 1: Getting Started

1. Network Security Monitoring Rationale · PDF · Keynote
2. Collecting Network Traffic & 3. Standalone NSM Deployment · PDF · Keynote

Part 2: Security Onion Deployment

We'll skip chapters 4 and 5

4. Distributed Deployment
5. SO Platform Housekeeping

Tools

6. Command Line Packet Analysis Tools · PDF · Keynote
7. Graphical Packet Analysis Tools
8. NSM Console · PDF · Keynote

NSM in Action

9. NSM Operations · PDF · Keynote

Projects (In Development)

Download VMware Player (64-bit)

Do Either One of These Projects

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Project 1: Setting Up Security Onion on a Mac (15 pts)
Project 1: Setting Up Security Onion on a PC (15 pts)

Project 2: Wireshark (15 pts. + 20 pts. extra credit)
Project 3: Splunk (20 points)
Project 4: Detecting Ransomware with Splunk and Sysmon (20 pts.)
Project 5: Command-Line Tools (15 pts.)
Project 6: Graphical Tools (15 pts.)
Project 7: NSM Consoles (15 pts.)

Extra Credit Projects

Project 1x: Setting Up ELK without SSL (15 pts. extra credit)

> Original Project 1x: Setting Up ELK -- Unnecessarily Complicated

Project 2x: CanaryTokens (5 pts. extra credit)
Project 3x: Splunk Searching (10 pts. extra credit)
Project 4x: Splunk Enterprise Security (10 pts. extra credit)
Proj 5x: Wazuh 3 Setup (15 pts.)
Proj 6x: Monitoring File Integrity with Wazuh 3 (15 pts.) (rev. 12-30-17)

Skip This Project

This project is frustrating and difficult. I'm only leaving it here for students who are already working on it. I think QRadar Community Edition is not yet ready for use. Use OSSEC instead for now.

Project 5x: QRadar Community Edtion (15 pts. extra credit)

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Links

Links for Lectures

Ch 1a: Working with Bro Logs: Queries By Example
Ch 1b: Monitoring HTTP Traffic with Bro -- Bro 2.5.1 documentation
Ch 1c: testmyids.com - Robtex
Ch 1d: Sguil - Open Source Network Security Monitoring
Ch 1e: Security Onion 14.04 Release Notes -- Snorby is Gone
Ch 1f: How can I install Snorby on Security Onion 14.04?

Ch 6a: Best Practices -- Security-Onion-Solutions/security-onion Wiki

Ch 7a: splunk pricing - splunk licensing model

Ch 9a: Mandiant APT1 Report
Ch 9b: VERIS Incident tracking

Other Links

SELKS 2.0 vs. Security Onion
How To Install Elasticsearch, Logstash, and Kibana (ELK Stack) on Ubuntu 16.04
Monitoring Windows Logons with Winlogbeat | Elastic
Using ELK for Logging on Windows: Configuration
Public PCAP files for download
SecRepo - Security Data Samples Repository
Xplico Graph not working properly
How You Can Set up Honeytokens Using Canarytokens to Detect Intrusions
Splunk Dashboard Examples | Splunkbase

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Tracking Hackers on Your Network with Sysinternals Sysmon
I've lost my splunk admin password, can it be recovered? - Question | Splunk Answers
Digital Corpora
NetworkMiner - The NSM and Network Forensics Analysis Tool
NetworkMiner packet analyzer - Browse /networkminer at SourceForge.net
How to Install Cacti 1.1.10 on Ubuntu 16.04
QRadar Rule creation: Baseline of trusted users - YouTube
Manage common offenses detected by QRadar SIEM
IBM Knowledge Center - Installing Sysinternals Sysmon

New Unsorted Links

Using Wazuh to monitor Sysmon events - WAZUH's blog
Splunk Book | Splunk
Wazuh v3.0 released!
Splunk Courses for Users
Get started with Search - Splunk Documentation
Splunk and the ELK Stack: A Side-by-Side Comparison
What on earth is 'Splunk' -- and why does it pay so much? (from 2017)
Splunk in 2 Charts: 85 of the Fortune 100 companies use Splunk (from 2017)
2018-11-26: Splunk Core Certified User Test Blueprint

Last Updated: 12-30-17 3:21 pm

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD