CS 6262 Recommended Readings

Recommended Reading for Lesson 1:
The DDOS that almost Broke the Internet
Practical Network Support for IP Traceback
A DoS-limiting Network Architecture

Recommended Reading for Lesson 2:
Spamalytics: An Empirical Analysis of Spam Marketing Conversion
PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs

Recommended Reading for Lesson 3:
The Hacker Playbook – Practical Guide to Penetration Testing, by Peter Kim

Recommended Reading for Lesson 4:
A Look Back at "Security Problems in the TCP/IP Protocol Suite"
Steve Friedl's Unixwiz.net Tech Tips: An Illustrated Guide to the Kaminsky DNS Vulnerability
BGP Security in Partial Deployment

Recommended Reading for Lesson 5:
Securing Frame Communication in Browsers
The Security Architecture of the Chromium Browser
Exposing Private Information by Timing Web Applications
An Introduction to Content Security Policy
Play safely in sandboxed IFrames
The Basics of Web Workers
Using CORS
Secure Session Management With Cookies for Web Applications
Origin Cookies: Session Integrity for Web Applications
ForceHTTPS: Protecting High-Security Web Sites from Network Attacks
Towards Short-Lived Certificates

Recommended Reading for Lesson 6:
Ether: Malware Analysis via Hardware Virtualization Extensions
Automatic Reverse Engineering of Malware Emulators
Exploring Multiple Execution Paths for Malware Analysis
Jekyll on iOS: When Benign Apps Become Evil
On Lightweight Mobile Phone Application Certification
Mitigating Android Software Misuse Before It Happens

Recommended Reading for Lesson 7:
BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation
BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection
Modeling Botnet Propagation Using Time Zones

Recommended Reading for Lesson 8:
ZMap: Fast Internet-Wide Scanning and its Security Applications
Building a Dynamic Reputation System for DNS
Detecting Malware Domains at the Upper DNS Hierarchy
The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers
Beheading Hydras: Performing Effective Botnet Takedowns

Recommended Reading for Lesson 9:
Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction

Recommended Reading for Lesson 10:
~~Tom Mitchell, Machine Learning, McGraw-Hill, 1997~~
Machine Learning for Humans – Parts 1, 2.1, and 2.2
A Framework for Constructing Features and Models for Intrusion Detection Systems
Anomalous Payload-based Network Intrusion Detection
Polymorphic Blending Attacks
Misleading Worm Signature Generators Using Deliberate Noise Injection

Recommended Reading for Lesson 11:
Secure and Flexible Monitoring of Virtual Machines
Lares: An Architecture for Secure Active Monitoring Using Virtualization
Secure In-VM Monitoring Using Hardware Virtualization
Inference Attacks on Property-Preserving Encrypted Databases
Practicing Oblivious Access on Cloud Storage: the Gap, the Fallacy, and the New Way Forward
Additional papers referenced in Lesson 11:
Practical Oblivious Storage
Oblivistore
Path ORAM
Oblivious RAM Simulation with Efficient Worst-Case Access Overhead

Recommended Reading for Lesson 12:
How to Share a Secret
Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance