

CS 4353 - Unix and Network Security

Instructor:

Hugh B. Maynard

4.01.28 SB

458-5542

Office Hours: 9:00 - 10:00 MWF

Text: **The Tao of Network Security Monitoring**

by Richard Bejtlich

Network Intrusion Detection - An Analyst's Handbook

by Northcutt and Novak

Prerequisites: CS 3433 (Computer and Information Security)

Topics:

- Computer Security and Ethics
- Minimal Linux System Administration
- Network Basics
- Review of Basic Open Source Security Tools
 - Tcpdump
 - Nmap
 - Wireshark
 - Tcpflow
- Packet Analysis
- Forensics
 - Network Flow Analysis
 - File System Analysis
 - ATA issues - HPA, DCO, hdparm, recovery, zeroing
 - The Coroner's Toolkit
 - Unix Command-Line Analysis
 - Sleuthkit
- Building Security Tools - Libpcap/Libnet/Libdnet
- More Wireless Security (or Insecurity)
- Web Insecurities

Grading:

Projects: 100 points

Tests if necessary (meaning do the projects carefully)

Total: 100 points

Grading Scale:

A: 90 to 100

B: 80 to 89

C: 60 to 79

D: 50 to 59

F: 0 to 59

Note: I reserve the right to lower the grading scale if necessary so that I can increase the difficulty of the projects.

Drop dates: The deadline for dropping without a grade assigned is January 28. The deadline for dropping an individual course is March 23.

Final Examination: 7:30 am - 10:00 am Wednesday, May 6.