Semester: Spring 2020

Course Format and Credit Hours: 3 hr Lecture, 3 hr Credit

Pre-requisites: Student should be knowledgeable in a high level language as well as assembly language, have computer architecture or computer organization background, and knowledge of TCP/IP such as a class such as CS-453.

Co-requisites: none

Instructor: Dr. Roy S Nutter, Office: 257 AEB
Tel: 304-293-9131
E-mail: rnutter@wvu.edu

Schedule: 10-10:50 MWF

Location: 215 ESB
Labs will be in the West Virginia Cyber Crime Cooperative (WV3C) facility, Suite 3102 (Prete Bld), 3040 University Ave, Morgantown, WV

Office Hours: MWF 2-3 or by appointment (best to call or e-mail me to be sure I will be there.)

Description: This course is an introduction to threat assessment in modern networked computer systems; and the techniques, methodologies and technologies for preventing intrusions, detecting intrusions, recovering from intrusions, and finally techniques for collecting evidence of intrusions.

“We assumed the digital footprints we left behind
our clickstream exhaust, so to speak--
were as ephemeral as a phone call, fleeting, passing, unrecorded.
...Our tracks through the digital sand are [in fact] eternal.”


© Roy S. Nutter, Jr, 2020
Objectives: The objective of this course is to provide students with a comprehensive view of the threats for networked computer systems, the various tools and technologies for protecting the network, techniques for emergency response, and, finally, methods to gather evidence.

Course Objectives: This course is to serve as an overview course of network forensics.

Expected Learning Outcomes: Upon successful completion of this course:

- The Student shall be able to
- Describe computing network architecture, components and their functions
- Describe network protocols, their uses, and vulnerabilities
- Apply protection measures against various network protocol attacks and other malicious code.
- Plan, implement and assess security protection mechanisms in generic computer and communication systems.
- Describe the various alternatives for firewalls, intrusion detection, trace-back and evidence gathering systems.
- Demonstrate a number of tools used in network forensics.
- Demonstrate the ability to investigate the occurrence, identification and source of break-ins by examining computer logs and other traces left in compromised digital networks.

Texts used (not required):

1. “Computer Forensics Investigating Network Intrusions and Cybercrime” by Cengage
2. “Network Forensics, Tracking Hackers through Cyberspace,” by Sherri Davidoff and Jonathan Ham,
   ISBN-10: 0-13-256471-8
4. “Guide to Firewalls and Network Security” by Michael Whitman, Mattord, Austin, and Holden
   ISBN-10: 1-4354-2016-0
Grading: Semester grades will be computed as follows:

- Presentations: 60%
- Presentation slides and written documentation including references for each presentation: 10%
- Attendance: 5%
- Final Project Report: 25%

TOTAL 100%

Grade Assignment:
- A= 90-100
- B= 80-89
- C= 70-79
- D= 60-69
- F= 59 and below

Grading Policy:

We may discuss vulnerabilities in widely deployed computer systems. This is NOT an invitation to exploit those vulnerabilities. Responsible behavior and avoidance of all unethical behavior is expected. WVU’s policy (and our own) on this is clear: you may not break into machines that are not your own. In addition to an F in the course and WVU proceedings under the Student Code of Conduct, legal proceedings and legal penalties may be brought against you for such actions.

Class Communications:

All class communications will be via ecampus.wvu.edu

Class Cancellations:

If a class is cancelled, notice will be posted on e-campus and mailed to your MIX ACCOUNT. Students are responsible for getting cancellation information and assignments. In all emergency situations, however, we rely on individuals to make the best decision for themselves about their safety.

Topical Outline
Introduction, What is Network Forensics

TECHNICAL FUNDAMENTALS
Review of TCP/IP (2)
  V4 and V6

TRAFFIC ANALYSIS
  Network Forensics and Logs (1)
  Investigating network Traffic (1)
  Investigating Web Attacks (1)
  Router Forensics (1)
  Investigating DoS attacks (1)
  Network Vulnerabilities (3)
    Port Scanning (2)
    Enumeration (2)
  Wireless Networks (2)
  Firewall planning and Design (3)
    Packet Filtering (3)
  Proxy Servers and App level Firewalls (3)
    Firewall configuration and Admin (3)
  Encryption and Firewalls (3)
  Setting up a VPN (3)
  Intrusion Detection and Prevention Systems (3)
  Network Protection Systems (2)
  Lab Final Project

© Roy S. Nutter, Jr, 2020