

# Resources and Assignments for MNGT6040/5040 Network Security class

To learn to implement security; not to be a hacker

## 1. Books:

- a. *A Manager's Guide to Network Security* by Carr & Snyder
- b. .PDF articles on *Social Engineering and Security* (emailed)
- c. *Computer Security Fundamentals* by Chuck Easttom, ISBN 0-13-171129-6
- d. *The Art of Intrusion* by Mitnick and Simon ISBN 0-7645-6959-7 (Optional)
- e. Security+ study guide

## 2. Classes

- a. **Tuesdays:** Lectures
- b. **Thursdays:** Lab sessions; Hands-on network assignments from lab manual.
- c. **Project Honeypot** = participation = 20% of grade
  - i. Set up email accounts on Hotmail.com; Go to websites and signup using this account
  - ii. Honeypot: Set up a computer to be connected to Internet on a student's cable or DSL modem without a router; without virus or other protection and no filtering; this will be home to hotmail account. Leave it open long enough to get stuff.
  - iii. Bring computer to Lowder #024; no connectivity; open emails
    - (1) Categorize email; is it just spam; phishing; carry virus
    - (2) Determine true source and spoofed source; alert switching stations
    - (3) Determine what attachments; what objective.
    - (4) Determine if have been added to a BotNet; Open client.
  - iv. Put a completely unprotected, unpatched machine on the University network to show just how vulnerable they are even in a relatively controlled environment.

## 3. Mid-term Exam - 15% of grade

## 4. Assignments - 5% of grade

## 5. Individual/team Project -

- a. Create a list of security subjects
- b. Each person will choose a topic and create a paper on it; no duplicates
- c. Papers will be shared with all other persons for critique.

## 6. Class paper: Whole class will participate on a network security and social engineering paper to be distributed to all of CoB

## 7. Final Exam - 10% of grade - Security+ Certification; passing = 100; not passing = 60.

## 8. Assignments:

- a. Do a reverse DNS of an IP address at [www.samspace.org](http://www.samspace.org).
- b. Use the program \_\_\_\_\_ and view all header information for a spam email from honeypot & Carr's CD
  - i. Who from; who really from; what IP address.
- c. Take a phishing email from honeypot and describe the techniques used, social and other

## Schedule of Lectures (Tuesdays)

MGNS = *A Manager's Guide to Network Security*; CSF = *Computer Security Fundamentals*

May 24	CSF 1; MGNS 1-20; homework = one page on Social Engineering; be prepared to discuss case on pg 26
May 31	CSF 2; .pdf on OSI levels for security; review IP addressing
June 7	CSF 3, tools; CSF 5, viruses
June 14	Jack Lawton ½ day on NAMS/CoB; MGNS pg 21-70; CSF 7, Encryption & CSF 10 Cyber Terrorism
June 21	Tom Marshall ½ on Database Security
June 28	<b>Bliss Bailey</b> on AU networks w/VLAN
July 5	Brandon Rogers, <i>IronMail</i> ® ½ day
July 12	Clif Fisher ½ day; CSF 9; homework = Create assess identification list for lab (CSF pg 222)
July 19	MGNS Wireless
July 26	
Aug 2	End of Classes: Final Exam = turn in Security+ exam

1. Introduction to Cyber Crime and Security.
2. Networks and the Internet.
3. Assessing a Target System.
4. Denial of Service Attacks.
5. Malware.
6. Basics of Assessing & Securing a System.
7. Encryption.
8. Internet Fraud, and Cyber Crime.
9. Industrial Espionage.
10. Cyber Terrorism and Information Warfare.
11. Cyber Detective.
12. Security Hardware and Software.

## Schedule of Labs (Thursdays)

May 26	Familiarity of how to secure individual machine; fix a machine in lab & YOUR machine. CSF 6 & ex 8.1
June 2	Familiarity with Command line; set up server as target of Ping of Death
June 9	Tools referenced in CSF chapter 3; get tools, including Wild Packets
June 16	Perform Ping DoS (exercise 4.1); determine how to fix server to protect from DoS (Ref CSF 4, ex 6.1,5)

CSF Table of Contents

June 23  
June 30  
July 7  
July 14  
July 21  
July 28

Write to author of CSF @ [chuckeasttom@yahoo.com](mailto:chuckeasttom@yahoo.com)

Risk Assessment - Disaster Planning  
Network Security  
Parameters of a Valuable Network  
Power for Network Equipment  
Security Issue Threats and Responses  
Prevention Measures  
Case 1 - Disaster Recovery  
Case 2 - Eight Ways to Protect Your Computer  
Top Five Online Scams (Yahoo) - Dan Tynan  
Wireless Network Security  
The Four Major Mistakes  
What Do Hackers Want?  
How Hackers Attack the Wireless Network  
Rogue Users  
Wireless Security Features  
Defensive Strategies  
Human Error and Network Administration  
Legal Implications  
Data Communications Certifications Available  
Case 3 - Best Practices for Wireless Network Security  
Case 4 - Next-Generation Virus Defense

NMGS Table of Contents