Week One

4 hr Agenda

8:00 –8:15		Classroom Opens (Rm. 202)
8:15 – 8:45		Overview/Class Expectations
Mod 1	Mod 1-1A	Introduction: Threats, Vulnerabilities, and Risks 70
	Mod 1-1B	*Knoppix Intro, Ethereal demo* Lab 1B1 Gathering WHOIS with Linux Lab 1B2 DNS Interrogation with Linux Lab 1B3 Network Reconnaissance with Linux *95 – 155 Min*

Week Two

8 hr Agenda

8:00 –8:15		Classroom Opens (Rm. 202)
Mod 2	Mod 1-2A	Management Practices 73
	Mod 1-2B	Lab 2A-1 Port Scanning Utilities for Windows Lab 2A-2 Active Stack Fingerprinting Using Windows Lab 2A-3 Enumeration Using LANguard in Windows Lab 2A -4 Generic Enumeration Using Windows Lab 2A-5 SNMP Enumeration Using Windows Lab 2B -1 Scanning Utilities Using Linux *110 -- 190 Min*
12:00 – 1:00		Lunch
Mod 3	Mod 1-3A	Access Control 71
	Mod 1-3B	Baseline System (*GSEC Baseline*) Lab 5A-1 Malicious Code Management and Hoaxes Lab 5A-2 Windows Log Analysis Lab 5B-1 Linux Log Analysis *60 – 95 Min* Online Knoppix Tutorial Demo (http://www-106.ibm.com/developerworks/linux/library/l-roadmap.html)

Week Three

8 hr Agenda

8:00 –8:15		Classroom Opens (Rm. 202)
8:15 -- 10:30	Mod 1-4A	Telecom and Network Security One 99
Mod 4	Mod 1-4B	Advanced Ethereal (packet analysis) demonstration. Sample Ethereal Labs from Computer Networking: A Top Down Approach
12:00 -- 1:00		Lunch
Mod 5	Mod 1-5A	Telecom and Network Security Two
	Mod 1-5B	Lab 5A -3 Traffic Analysis Using Windows Lab 5B – 2 Traffic Analysis Using Linux *35 – 60 Min* *Ethereal/TCPDump/Nmap Lab from presentation?*

Week Four

8 hr Agenda

8:00 –8:15		Classroom Opens (Rm. 202)
Mod 6	Mod 1-6A	Cryptography, 92
	Mod 1-6B	PGP Lab Old Exercise 5-6 Password and Password Policy Evaluation (*GSEC Supplement?)* Demo Lab 7A-4 Digital Certificates with Microsoft Certificate Authority 20 -- 35 Min
12:00 -- 1:00		Lunch
Mod 7	Mod 1-7A	Operations Security 42, Security Architecture 67
	Mod 1-7B	Lab 7A-1 Windows Access Control/Encryption 20--35 Min Lab 7A-3 Web Browser Security and Configuration (IE) 20 -- 35 Min Demo Lab 7A-5 Remote Connectivity with Microsoft RRAS 20-35 Min *60 – 105 Min*

Week Five

Open Lab

9:00 – 2:00	Open Lab	Prepare Projects and Presentations

Week Six

8 hr Agenda

8:00 –8:15		Classroom Opens (Rm. 202)

Mod 8	Mod 1-8A	Applications and Systems Development (30), Business Continuity Planning/Disaster Recovery (56)
	Mod 1-8B	*Selection from:* *Lab 3A-1 Windows 2000 Vulnerabilities 60-75 Min* *Lab 3A-3 MBSA 20 - 35 Min* *Lab 3A-4 NetBus 30 – 45* *Lab 5A—1 Malicious Code Management and Hoaxes 25 – 35 Min* *Lab Manual, Exercise 4A-1, Firewalls 25 – 40 Min* *Lab Manual, Exercise 4A-3, File Integrity Monitoring with LanGuard 30 – 35 Min* *Exercise 5A-2, Windows Log Analysis 20 – 35 Min* *210 -- 300*
12:00 -- 1:00		Lunch
Mod 9	Mod 1-9A	Law, Investigations, and Ethics (61), Physical Security (33)
	Mod 1-9B	Lab 7B-1 Linux File System Access Control 20 – 35 Min Lab 7B-2 Web Browser Security and Configuration (Mozilla) 20 – 35 Min Lab Exercise 8, Introductory Forensics Demo *Exercise 3-5a, Unix/Linux Vulnerabilities and Protections (John)* *CyberProtect Simulation? Log Analysis, Zone log uk, Proximon?*

Week Seven

4 hr Agenda

Mod 10	Mod 1-10A	Presentations
	Mod 1-10B	Final

Notes

One All projected lab times are based upon the assumption that students are properly prepared. At a minimum, this means reading the relevant text prior to class. It may also mean researching the day's labs and reviewing past work.

Two This is a dynamic class. It is likely that, as the class progresses, this agenda will change. It would be good policy to pay attention in class when we announce the next week's agenda.

Three Labs will be taken from the text as well as from other references. These other references likely will included:

Cole,E, et. al., SANS GIAC Certification: Security Essentials Toolkit (GSEC), Que, ISBN: 0789727749

and

Kurose, J. and Ross, K, Computer Networking : A Top-Down Approach Featuring the Internet, Addison Wesley, ISBN: 0321227352