**Week 1 –Security Overview**

•Be able to define the important security concepts

•Be familiar with the core security principles

•Phishing/Email Header Analysis

•Understand how the BeEFlab worked

•Be familiar with how Tor works

•Common 5 Phases of an Attack and their defenses

•Understand the Recent Popular Security Threats

Review:

•What is non-repudiation?

•Main method to verify file integrity?

•Name some examples of inside threats

•Name some examples of outside threats

•Last phase of an attack

•Common defenses against elevating access?

•What defense in depth step is often missed?

•Shellshock is a vulnerability in what?

**Week 3 –Malware Overview & Exploit Kits**

•Be familiar with all malware types listed in the slides, their propagation methods, and common payloads

•Understand how botnets work

•Understand how Netcat backdoors work

Be able to pick the correct commands out of a list

•Understand basic malware detection and remediation techniques

•Understand the general chain of events and goal of web exploit kits

•Know the details about how Crimebossand Blackhole work, payloads and signatures they use, etc.

•Understand how Wireshark is organized and how it was used in the lab

•Understand details about what the Crimeboss exploit kit did in the packet capture from the lab

Review:

* Why does the Conficker worm use IP address querying sites to collect the IP address of the infected victim?

**Week 4 –Malware Analysis**

•Understand steps for creating an isolated analysis environment

•Understand all types of static and dynamic malware analysis

•Understand what each analysis tool does, how it is used, and what type of malware analysis it performs (static or dynamic)

Be able to identify the tool based on a screenshot

•Understand what happened in the Windows Live Messenger lab

•Understand levels of abstraction

**Week 5 –Attack Vectors & Mitigation Techniques**

•Understand attacker taxonomy

•Understand types of social engineering attacks

•Be familiar with how the mentioned network protocols work

•Be able to identify DoS/DDoS attacks based on seeing screenshots of packet captures

•Be familiar with how buffer overflows work as well as the code involved (such as the in-class lab)

•Understand how ARP Poisoning works and how to use arpspoof and the tools we used in class

Be able to pick the correct command out of a list

Be familiar with the diagrams

•Understand the defenses against the various attacks

**Week 6 –Web App Attack Vectors & MitTech I**

•Be familiar with the first three of the OWASP Top 10 (Injection, Broken Auth/Session Mgmt, XSS)

How each attack works

Goal of attacks

Defenses against attacks

Be able to identify an attack based on seeing a screenshot of a webpage

•Be able to identify correct database SQL queries out of a list

•Make sure you can identify correct SQL or OS injection queries out of a list

•I would be familiar with most all topics in the week 6 slide deck

**Week 7 Web App Attack Vectors & MitTech II**

•Be familiar with the remaining categories of the OWASP Top 10

How each attack works

Goal of attacks

Defenses against attacks

Be able to identify an attack based on seeing a screenshot of a webpage

•Understand the difference between LFI, RFI, and Directory Traversal

•I would be familiar with most all topics in the week 7 slide deck