Information Assurance
Final notes
Spring 2006

This note is intended to help you prepare for the information assurance final exam. The exam will be more challenging than the midterm was.

Please refer to the notes I provided about the midterm, as the recommendations for study are the same.

Topics and expectations

- I expect you to know all the material as listed on the midterm notes.
- Be aware of different types of malicious logic, both threats from malicious insiders, and from external malicious code.
- Understand how viruses are constructed and spread, and how they can be detected.
- Understand what defenses are possible against malicious code.
- Understand and be able to describe and diagram how buffer overflows occur.
- Understand and be able to recognize errors in software that can lead to vulnerabilities.
- Be able to describe what problems malicious programmers can cause if they are on a development team.
- Understand and be able to describe a variety of mechanisms that prevent buffer overflows or make them more difficult.
- Understand the different forms of input to an SUID program that exist on a UNIX system, and be able to describe the various ways that an attacker can use these to attack the program or system.
- Understand and be able to describe the various forms of output that an SUID program can produce, and how these can be subverted by an attacker to affect the system.
- Understand what can be done to preserve the integrity of files in a file system.
- Be familiar with the basic logs in a UNIX system.
- Understand and be able to diagram and explain the anatomy of an audit system, and be able to explain the functions of the component parts.
- Be able to explain what information might be in a log file, and why and how that file might be sanitized before being made available to outside entities.
- Understand each of state-based and transition-based audit systems, and be able to contrast the two.
- Understand and be able to describe the function of various network hardware components, such as a switch, router, firewall, and NID systems.

- Know and be able to describe how ARP cache poisoning occurs. Understand what DNS cache poisoning is.
- Understand and be able to describe and diagram simple attacks against network routing, such as black-hole routing.
- Be able to describe how IPSec works and what the various headers do and what risks they protect against.
- Be able to describe what IP spoofing is, and tell what threats arise from it.
- Understand and be able to describe ingress and egress filtering.
- Understand and be able to describe what blind IP spoofing is. Also be able to describe what TCP session hijacking is and how it can be detected. Be able to describe how source routing can be used to spoof IP addresses.
- Be able to describe various methods by which a denial-of-service attack can occur.
- Understand and be able to describe how attackers on the internet can hide their true location. Describe the problems that need to be solved to be able to locate them.
- Understand the various types of firewalls, and be able to diagram different common network configurations for firewalls.
- Understand how intrustion detection systems work. Be able to contrast host-based and network-based systems. Be able to contrast signature-based systems from anomaly-detection systems. Understand and be able to describe some methods that attackers can use to thwart a network intrusion detection system.
- Know what actions to take when a system is compromised, and what your legal options are in that case.
- Understand and be able to describe what forensic information may be left on a system. Be also to define and describe what slack space is, and how deleted files might be recovered. Be able to list the general steps in taking forensic evidence.
- Be able to answer questions regarding common themes in the bugtraq and RISKS mailing lists. In specific, be familiar with the material posted in the Bugtraq presentations.