Tufts University
Department of Computer Science
COMP 116: Introduction to Computer Security
Fall 2013
Final Examination Information. Thursday, December 5th in class.

Topics:

- Networking and packet analysis
- “Thinking like a bad guy” / reconnaissance / security policies
- Network scanning
- Network sniffing
- Spoofing
- Hijacking
- Web security / SQL injection / Cross-Site Scripting (XSS) / cookie tampering / command injection
- Cryptography / symmetric algorithms / asymmetric algorithms / hash functions / password cracking
- Privacy
- Static analysis
- Risk management and analysis
- Buffer overflow
- Incident handling
- Forensics
- Anti-forensics
- Legal issues
- Malware / viruses / worms / backdoors / tini / netcat

What is the point of a final exam in this class?
General security literacy in a broad sense.

Why a closed book exam?
If I make it an open book exam, then what is the point of the final exam (see above)? Also, so you don’t waste time as you only have an hour-and-fifteen minutes to complete it.

Format:
The final exam for this class on Thursday, December 5th is closed book but you are allowed to bring one 8.5”x11” cheat sheet (yes, you can use both sides). It will contain at most 4 questions. One of the question will be scenario-based. Another question will be a series of short answer questions, including true-false types. Fill-in-the-blank and multiple choice type questions will not be on the exam.

The Open Question:
One of the questions will be one of the following, exact wording. I will not tell you which one will

be on the actual final exam. Rules:

- You may use any printed or web materials to solve a problem.
- You should develop a strategy to solve each problem. I urge you to do all problems (i.e., program, implement) to prepare for the final exam.
- Collaboration among class members is encouraged between now and the real final.
- Collaboration with other persons outside the class is prohibited.
- You may not ask me for help other than for clarification purposes.

1. Multi-tiered architecture is a client-server architecture that is accepted in network security. The most popular multi-tier architecture, especially in the enterprise, is the three-tier architecture. Describe two benefits and drawbacks of multi-tiered architectures.

2. The vulnerability window for a 0day attack is the time between when a vulnerability is first exploited and when software developers start to develop a counter to that threat. Explain why it is difficult to measure the length of a vulnerability window for a 0day attack.

3. When acquiring data in a computer forensics investigation, explain why it is important to first determine whether or not a rootkit has been installed.

4. You are a manager at a prominent professional firm that specializes in enterprise risk, and advisory services. You receive a call from the CIO of a major client, a Fortune 500 company, regarding a spike in web traffic and unauthorized transactions over the past 48 hours. You will be leading the forensics investigation.

- Elaborate on the investigative procedures once you arrive on site prior to performing any analysis.
- How will the investigation be different if the client is a financial institution?
- A few days later in your analysis, you determined the cause of unauthorized transactions to be a cross-site request forgery (XSRF) vulnerability on the website. Briefly describe this vulnerability and give an example of how to exploit this vulnerability.
- What are some ways to prevent XSRF?

5. Identify the similarities and differences between the iOS and Android security models.