Review questions for final

Questions on various types of malware and defenses

- Why is the C function gets() inherently insecure?
- Why is C more vulnerable to buffer overflow attacks than python, perl, or other higher level languages?
- Describe how a stack overflow attack is executed.
- What is a heap overflow attack?
- What does fuzzing mean?
- What is chroot jail?
- What is a no execute bit, and how does it work? Name one type of overflow attack this won't help against.
- What is address space layout randomization, and why is it used?
- What is a canary? What types of attacks or errors won't they help defend against, and why?
- Give an example of a simple SQL injection attack. What are the common ways to defend against these?

Questions on wireless and networking issues

- How does TLS work to layer security onto inherently insecure HTTP protocols? Give at least two ways it might fail to work.
- How does DNSSEC work, and what does it protect (and not protect) against? Where is it supported, and why doesn't everyone use it?
- Describe the purpose of onion routing, and briefly explain how it works.
- Why is WEP not considered secure at this point, and how does WPA address those issues?
- What is the Guninski attack?
- Give two security issues that come up immediately with the use of cookies.
- Describe how cross site scripting works, and how programs can defend against it.

Questions on access control

- What is 2 factor authentication?
- What is the simple security property in the Bell-Lapadula model? What is the *-property? How do these work together to ensure data integrity? What is the ds-property?
- How does the Biba Integrity model differ from the Bell-Lapadula? What are the 3 rules in this system (analogous to the ones in the previous problem)?

- What is the Clark-Wilson integrity model designed for (as opposed to the Biba and Bell-Lapadula models)? What are the two main concepts in this model?
- Describe the Chinese wall model, and give an example of where it might be used.

Questions on OS security

- What type of access control does Linux generally support, and what impact does this have on security?
- When securing a computer system, why do we limit how many applications are running?
- What is chroot jail?
- How are mandatory access controls implemented in Linux?
- What is SELinux?
- Briefly describe the functions of the following components on a Windows machine: Security reference monitor, local security authority, and security account manager
- Give one reason local accounts can be better than domain accounts, and one reason why domain accounts may be preferable to local accounts.
- How is mandatory access control implemented in Windows?
- What are the governing principles of hardening systems in Windows? How and why are these different than the main principles in Linux system design?
- How does windows prevent against buffer overflow attacks? What about heap overflow attacks?
- What is a no execute bit, and how does it work? Name one type of overflow attack this won't help against.
- What is stack randomization?
- What features does a ”trusted” OS add to operating systems functionality?
- Describe what is meant by terms such as “kernalization” and “virtualization”, and give examples of where each has been implemented.
- What is the orange book, and what are the classifications it provided? What were some of the inherent flaws that led to disuse of its system?
- How does the Common Criteria, and how does it classify trusted systems?

Questions on logging and forensics

- What is computer forensics? What are the key elements used in computer forensics?
- What is the main balance to find in auditing or logging of data?
- Be able to analyze a small log file to determine if some event occurred or explain an event (similar to the lab).

Questions on mobile security

- What types of attacks are unique to phones and mobile platforms?
- How does code signing differ between the android and the apple models?
- In the android platform, how do permissions differ from a traditional UNIX environment?
- In the android development context, what is an intent and why is it important from a security perspective?
- On the android model, why is the log cat utility so important from a security perspective?

Questions on intrusion detection

- Name and describe some types of distributed denial of service (DDoS) attacks.
- What is a honeypot?
- How do network intrusion detection systems work, and where do they monitor traffic?
- Compare the following intrusion detection strategies: anomaly-based, signature-based, specification-based, and behavioral based

Questions on database security

- In the context of database security, what is an inference attack? Give an example of what this means, and list a few common techniques that are used to defend against them.
- What is the difference between k-anonymization and differential privacy?

Random topics (not in one of the other groups above)

- What is DKM, and what is it used for?
- What protocols or features have been added on to SMTP in order to provide some security and authentication?
- What is TPM and trusted computing? What functionalities does it incorporate and where is it used?
- Why is TPM not perfect? (Related - what is an ”evil maid” attack?)
- What is a man-in-the-browser attack?
- What are some ways to combat the problem of spam emails?
- What is a PPI network, and why are they used?