CSS 337: Exam 2 Study Guide

1. What is reconnaissance? What are active and passive recon?
2. What is google hacking? Give examples
3. What are some examples of reconnaissance tools? What information do they provide? How can this information be used by a hacker?
4. What is a firewall? What are their benefits and limitations?
5. List three design goals for a firewall.
6. List four characteristics used by firewalls to control access and enforce a security policy.
7. What information is used by a typical packet filtering firewall?
8. What are some weaknesses of a packet filtering firewall?
9. What is an application-level gateway?
10. What are the common characteristics of a bastion host?
11. Why is it useful to have host-based firewalls?
12. What is a DMZ network and what types of systems would you expect to find on such networks?
13. How do you write firewall rule set? See class problems and assignment.
14. What are the limitations of intrusion prevention systems?
15. List and briefly describe the steps typically used by intruders when attacking a system.
16. Describe the logical components of an IDS.
17. Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?
18. What are three benefits that can be provided by an IDS?
19. What is the difference between a false positive and a false negative in the context of an IDS?
20. What are the differences between anomaly detection and signature based intrusion detection?
21. Learn all types of network attacks discussed in class – DoS (syn flood, ping of death), Spoofing, Sniffing, Man-in-the-Middle, TCP/IP hijacking, Phishing etc.
22. What is a malware? What are the different types of malware?
23. What are typical phases of operation of a virus or worm?
24. What are the functional components of a virus?
25. What mechanisms can a virus use to conceal itself?
26. How can viruses be classified based on target or concealment strategy?
27. What are macro viruses?
28. How does a Trojan enable malware to propagate? How common are Trojans on computer systems? Or on mobile platforms?
29. What is a “logic bomb”?

30. What is the difference between a backdoor, a bot, a keylogger and a spyware? Can they all be present in the same malware?
31. What are the differences between DAC and RBAC?
32. List and define the three classes of subject in an access control system.
33. In the context of access control, what is the difference between a subject and an object?
34. What is an access right?
35. What is the difference between an access control list and a capability ticket?
36. What is Attribute based access control? Explain in detail
37. What are the basic steps needed in the process of securing a system?
38. What is the aim of system security planning?
39. What are the basic steps needed to secure the base operating system?
40. Why is keeping all software as up to date as possible so important?
41. What are the pros and cons of automated patching?
42. What is the point of removing unnecessary services, applications, and protocols?
43. What types of additional security controls may be used to secure the base operating system?
44. What additional steps are used to secure key applications?
45. What steps are used to maintain system security?
46. Where is application and service configuration information stored on Unix and Linux systems?
47. What type of access control model do Unix and Linux systems implement?
48. What permissions may be specified, and for which subjects?
49. What effect do set user and set group permissions have when executing files on Unix and Linux systems?
50. Where is application and service configuration information stored on Windows systems?
51. How is a chroot jail used to improve application security?