This open-book examination is to take 120 minutes. Please answer exactly forty-five (45) of the forty-nine (49) questions presented below. Write an X through the number of any question not being answered.

You are allowed as much written or printed material (such as notes or books) as you want to use. No artificial magnification aids other than normal prescription glasses are allowed.

You may have one or two two-character codes for final exam extra credit. Write any such codes in the spaces indicated. Two points will be deducted from your final exam for any invalid code written in a space. Extra Credit Code 1: _ _   Extra Credit Code 2: _ _

Pledge (Must be signed according to UF Honor Code):
On my honor, I have neither given nor received unauthorized aid in doing this assignment.

____________________________________ (signature) ____________________________ (printed)

1. Why does the Apple App Store not have any third-party iPhone applications that can verify there are no malicious executable files on your iPhone?

2. What file can be modified on a linux host to toggle its behavior with respect to forwarding IP packets?
3. Why does the Smartphone Pentest Framework include a modem device for mounting attacks?

4. What IP packet field does traceroute successively modify in order to determine the number of hops to a specific host and what is the maximum number of hosts that can transfer an IP packet that reaches its destination?

5. What is the maximum prison term associated with violations of the Cyber Security Enhancement Act of 2002?
6. Consider the following password entry:

   $2a$07$b1b2ee48991281a439da2OHi1vZF8Z2zIA.8njYZKR.9iBehxLoIC

   What cryptographic hash was used to create this?
   What salt was used?

7. Briefly explain the significance of Sierra Corporate Design, Inc. v. David Ritz to the act of identifying hosts in a subdomain.

8. Suppose you try to use proxychains to forward traffic to a DNS server. Why would this fail?
9. What is CSRF? Name two measures to prevent CSRF attacks from succeeding.

10. Suppose you are trying to use arp spoofing to MITM an ssh session to server.somedomain.com from host victim.thisdomain.com on your local network segment. You send repeated gratuitous arp replies showing your MAC address is associated with both these machines' IP addresses. You know that a user on victim.thisdomain.com is trying to establish the ssh connection, but you never get any requests on port 22. What did you do wrong?

11. What kind of password can L0phtcrack crack?
12. How does the Veil framework help a penetration tester deploy software tools on a victim machine?

13. Cite two different reasons one might prefer to use a reverse-http meterpreter rather than a bind-tcp meterpreter payload in Metasploit.

14. Why can rainbow tables be constructed for NTLMv1 passwords but not for Linux passwords?
15. If I want to determine whether the ufl.edu domain has any BusyBox web servers running and I don't actually want to scan the ufl.edu servers, what resource could I use to find such machines?

16. If you have just compromised your first host (a linux machine) in a client's network and now have a root shell, what file should you download first to extend your access to the network?

17. Write a brief script that you could run on a windows machine in order to do a ping sweep of hosts on the local network. Assume the network address is 204.120.204.0/24.
18. What is the typical problem with code that causes a web application to be subject to SQL injection and how is this remediated?

19. Explain the plan for a MITM attack that downgrades Digest Authentication to Basic Authentication. Briefly describe each step in such an attack.

20. How can I use Burp Suite to overcome client-side javascript data sanitization? What browser reconfiguration is required?
21. How does CeWL increase your likelihood of finding relevant hostnames in a penetration test?

22. What mistake do many sites make w.r.t. listing URLs in their robots.txt file and how can such a mistake help attackers?

23. Why is it impossible to use Laudanum to execute a command with sudo?
24. Imagine a scenario with all class C networks. My attack machine is 128.227.162.167 and I have compromised Linux host 128.227.9.48. I want to use that host to contact port 21 on host 128.227.248.51. Assuming there are no firewall restrictions on high-numbered ports, explain how I can use netcat to arrange communication from my attack host to my ultimate target. Answer in the form of “On Host X execute command Y,” ….

25. How does a penetration test provide more information to a company than a vulnerability assessment using a tool like Nessus or Nexpose?

26. How does sslstrip steer traffic to the attack host and on what port does it provide a service?
27. Name two different sources for open source information that would be helpful to use in mounting a phishing exhibition.

28. What useful configuration information about a client's network might you find by looking at job listings?

29. Why is it a good idea to use more advanced banner grabbing features of nmap when identifying services rather than using RFC-specified mappings of open ports identified during a port scan?
30. Explain how it is possible that you may have compromised an Administrator account on a machine yet you cannot access remote shares that users on that machine *can* access.

31. Why are SMS attacks more common in eastern Europe that in the United States?

32. What potential negative outcome can result from starting a telnet server on a compromised host in a penetration test in order to be able to communicate with that host?
33. Give two reasons Powershell is an effective tool for delivering exploits to Windows 7 (and higher) hosts.

34. Name a situation in which you would be unable to conduct offline password cracking but might be able to mount an online password guessing attack. What countermeasure would make the online attack difficult?

35. How could a malicious hacker use Wigle.net's 10,000 top SSIDs to help MITM cell phone wifi connections?
36. What role does client deauthorization play in WPA PSK attacks?

37. What type of packet is replayed over and over by the FMS attack (and others) to target WEP? Why is this type of packet used and how is it identified?

38. Explain one method of making sure the Apple iTunes Store will not be able to use automated checks to discover the malicious behavior of exploit software.
39. Describe a situation in which it would be preferable to connect to a host with a reverse-http meterpreter rather than with VNC even if a target host has a VNC server running already.

40. Tell me what commands I might use to modify the firewall rules on a Windows host so that I can run a telnet server and connect remotely to it.

41. Explain how installing netcat on a machine that has no ports open to an incoming connection from an attack host might allow me to communicate to that machine from that attack host without modifying its firewall rules.
42. What does the meterpreter use in order to obfuscate communication between the attacker and victim machines?

43. What type of server must an attacker provide in order to capture credentials from WPA2/EAP users?

44. What countermeasures can be employed to avoid being attacked by a Pwnie Express device.
45. Identify several factors that explain why there is no encryption on the SS7 network.

46. What is WPAD and how does it make it easy for Responder to act as a MITM.

47. How many times must the krbtgt account password be reset in order to make a currently usable golden ticket no longer be useful?
48. Why is it unethical to perform a penetration test for a company to whom you provide protective security services or software?

49. Why is it useful to have a lawyer who is well versed in international law review your contracts even if you only perform penetration testing for U.S.-owned companies?