1. Select a web site.  
(1).

Use "Wget” or “Teleport Pro” to mirror the site. Look for comments within comment tags. Give screen dumps and explain what you found.

(2). Use“DirBuster” with a proxy feature through “privoxy” to enumerate hidden files and directories. Screen dump and explain the hidden files and directories you found.

2.(20 points) Lookup “How I met your girlfriend” in the BlackHat 2010 demo to explain, in 0.5 page, how this was done.  
3. (20 points) Select a person. Use on-line sites for phone book, social network, information, job, photo management, business directory, [jigsaw.com](http://jigsaw.com/), etc. to summarize, with screen dumps and explanations, what information you can get. If your target is not in US nor native English speaker, you might need to use on-line sites different from the textbook.  
4.(20 points) Google “XYZ resume firewall” and “XYZ resume intrusion detection” where “XYZ” is the name of your target company.  Screen dump “useful” results and explain what you got.  
5.(20 points) Lookup Archive.org and Google cached results, and select a target web site. Compare the differences between an archived and cached copy with its current on-line web site. Give screen dump and explain the differences.  
6.(20 points) Find Google Hacking Database at [hackersforcharity.org/](http://hackersforcharity.org/)ghdb/. Summarize what it has and select 3 strings to search. Screen dump and explain what you got.  
7.(20 points) Select a web site. Start from [whois.iana.org](http://whois.iana.org/) to find its registry, registrar, and registrant. Also select an IP address. Start from [arin.net](http://arin.net/) to find who owns the IP address. Show your screen dump and explain.  
8.(20 points) Select a domain name. Use nslookup to dump its DNS records. Show your screen dump and explain.  
9.(20 points) Select a domain name. Use traceroute or similar tools to find the access path to that domain. Show your screen dump and explain.  
10.(bonus: 40 points) Follow the case study right before chapter 1. Select one target and run through all tools (Tor, Vidalia, Privoxy, tor-resolve, proxychains, Nmap, socat, nc). Screen dump the process and explain what you got in your screen.