1.(30 points) Use all of WHOIS, Robtex, and PhishTank to trace back on a phishing email found in your mailbox. If you don’t find one, create one email account and post the email address onto Web to solicit some. Show and discuss your findings.

2.(30 points) On Windows with some running processes connecting to the Internet, use FTK Imager to dump memory and then Volatility Framework to analyze the memory dump. Show processes with connections, and check whether they have DLLs.

3.(30 points) Retrieve Poison Ivy RAT from the Internet. Use a program tracing tool you are familiar with to trace this RAT. Show how you trace the RAT with your tracing tool and summarize what modules this RAT contains.

4.(20 points) Use Nmap, NTA Monitor, IKEProbe to identify whether a target VPN server supports Aggressive mode. Screen dump “useful” results and explain.

5.(20 points) Use SiVuS, SIPVicious to scan a public SIP server. Screen dump “useful” results and explain.

6.(30 points) Setup your own client and an AP, or find an existing AP, running no encryption. Use wireshark or airodump-ng to sniff and decode data frames. Show and discuss your findings.

7.(50 points) Setup your own client and an AP to run WEP. Use the aircrack-ng suite to crack the WEP key by running through the steps of frame capturing, fake authentication attack, ARP replay attack, and key cracking. Show and discuss the steps you run through.