**14.2.8 Lab - Social Engineering**

a. What are the three methods used in social engineering to gain access to information?

Answer: Pretexting, Phishing and Spear phishing.

b. What are three examples of social engineering attacks from the first two methods in step 2a?

Answer:

+ The most common example of a pretexting attack is when someone calls an employee and pretends to be someone in power, such as the CEO or on the information technology team. The attacker convinces the victim that the scenario is true and collects information that is sought.

+ The user is redirected to a bogus page appearing exactly like the real renewal page, where both new and existing passwords are requested. The attacker, monitoring the page, hijacks the original password to gain access to secured areas on the university network.

+ Phishing emails are designed to appear to come from a legitimate source, like Amazon customer support, a bank, PayPal, or another recognized organization. Cyber criminals hide their presence in little details like the sender’s URL, an email attachment link, etc.

c. Why is social networking a social engineering threat?

Answer: Because social networking usually encourages people to share personal information along with interests and habits, cybercriminals can use it as a means to an end, gleaning personal information about you to use for malicious purposes. Hackers can use even the most innocuous information and smallest details you share to build a believable profile that can either be used on a social media network (to carry out some of the scams we’ve mentioned already) or elsewhere.