Discussion Questions for the Target Case Study

Answer the following questions for the Target data breach in 2013. You are encouraged to use diagrams and charts to illustrate your ideas.

For your reference, here is a government report on the Target breach.

* US Senate Report. A kill chain analysis of the 2013 target data breach, 2014.

Discussion Questions:

1) Use your own word to explain what happened in the Target data breach.

2) The HVAC contractor’s credentials were compromised by email phishing. Please propose at least two effective security mechanisms to guard against email phishing in the enterprise network.

3) If you are the hacker, please propose a scheme to launch phishing email attack at Target. Please be as detail and as realistic as possible.

4) These stolen credentials alone did not provide direct access to the company's point-of-sale devices. The hackers then acquired elevated rights that allowed them to navigate portions of company’s network and to deploy malware. This process is usually called Privilege Escalation. Name as many ways as you know to do Privilege Escalation.

5) To do privilege escalation, the hackers need to do vulnerability scanning on the Target network. Please propose as many ways as you know to do vulnerability scanning?

6) Most POS machines on the market nowadays run Microsoft Window OS, which is vulnerable to viruses and malwares. If you are the Target CTO, propose at least two measures to enhance POS security.

7) Target admitted that they ignored many alerts from their network security devices because of alert overload. If you are the Target CTO, what would you do to alleviate the problem of alert overload?

8) The security experts are criticizing Target for failing to isolate sensitive sections of their networks from those more easily accessible to outsiders. If you are the Target CTO, please propose a feasible solution to segment and categorize your networks and resources.

9) IT Weaknesses Paved the Way for Target Hackers. Please identify as many weaknesses as possible in the Target IT security.

10) If you are the CIO of Target, what would you do to improve IT security?