Readme File for Teachers:  
Case Study on Target Data Breach in 2013

**Abstract:**In this case study, students will look into the detail of the cyberattack on the Target Corporation in 2013. Students will learn how the attack take place from the beginning to the end. During the process of case analysis, a list of security topics reflecting different aspects of the breach is introduced. Through guided in-class discussion and hands-on lab assignments, student learning in lecture will be reinforced.

**Target audience:**Undergraduate, Graduate

**Objectives:**

* Describe real-world cyber breaches and how these breaches could have been prevented.
* Explain common offensive cybersecurity techniques, including email phishing, vulnerability scanning, and privilege escalation.
* Explain common cybersecurity defense techniques and common vulnerabilities
* Summarize how multiple security systems are integrated and how to establish a holistic view of cybersecurity in an enterprise environment.

**Keywords:**Target, email phishing, active persistent attack (APT), malware, POS

**Description:**The Target data breach started around late 2013 and became publicly known around Dec. 2013. Hackers gained access to more than 40 million credit and debit card information, plus 70 million personal information through malware on Target’s Point-Of-Sale (POS) systems. Target didn’t publicly release breach details, and probably will never do so. But enough information exists online and within the cybersecurity community to piece together what likely happened during the breach. These information can help people prevent similar attacks in the future. Figure 1 is a diagram illustrating the Target data breach with timeline. Information were collected through a number of sources (See Additional third-party resources for the case). In Figure 1, arrows with question marks represents details that are not fully revealed yet.

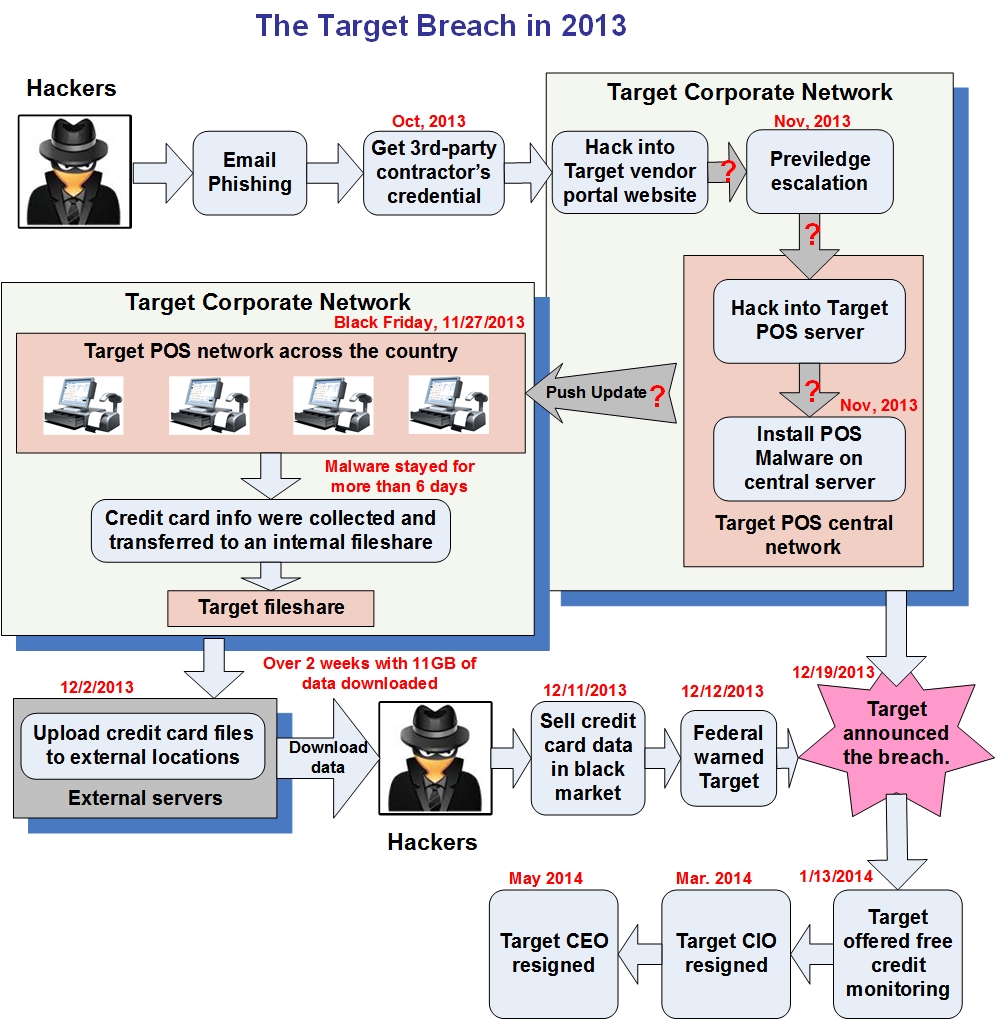


Figure 1: Target Data Breach

There are several reasons why we decide to use the Target data breach as one of the representative cases. First, the Target breach represents a typical type of cyber threats named Advanced Persistent Threat (APT). APT is a set of stealthy and continuous cyber hacking processes with the intention of stealing high-value data and information from targeted organizations. Second, the Target breach happened a few years ago, short enough so that lessons learned are not out-of-dated, also long enough so that there are sufficient details available to piece things together. Third, the Target breach is a high-profile case, which can easily draw students’ attention and interests.

There are two ways of using the Target case. First, we will have in-class discussion on the Target case during the semester. Students will answer questions and have discussions on the Target breach. Figure 2 is a list of sample discussion questions on the Target case. Second, we can use the Target breach as an example when teaching individual security topics. Figure 3 shows the corresponding security topics at the different stages of the Target case.

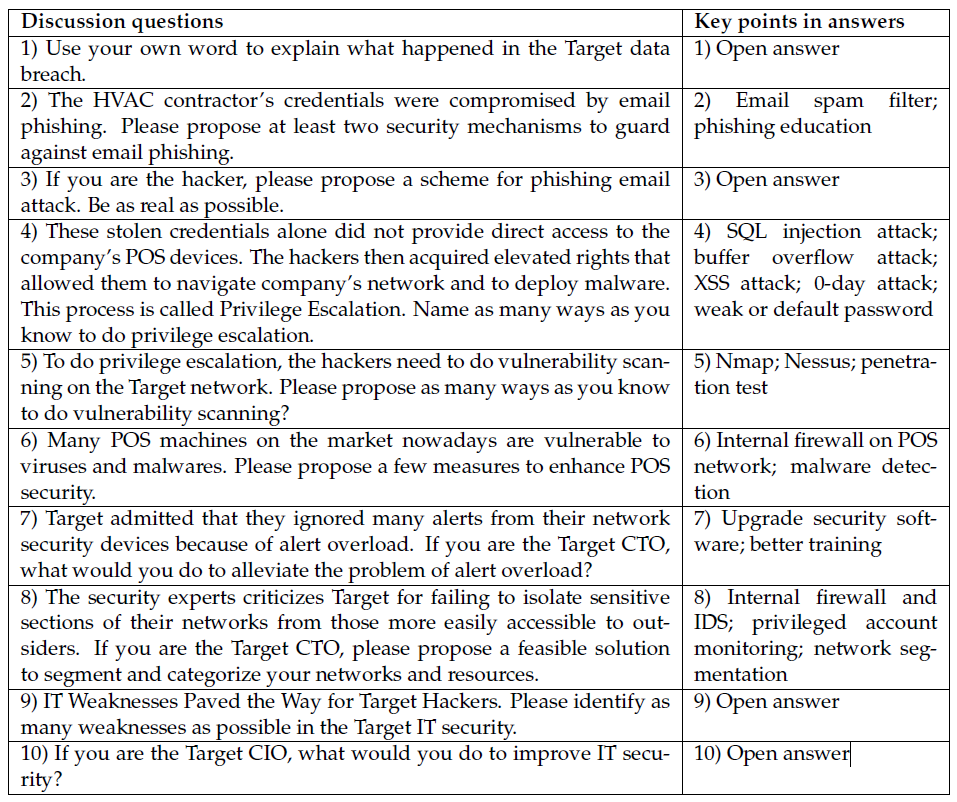


Figure 2: Discussion Questions

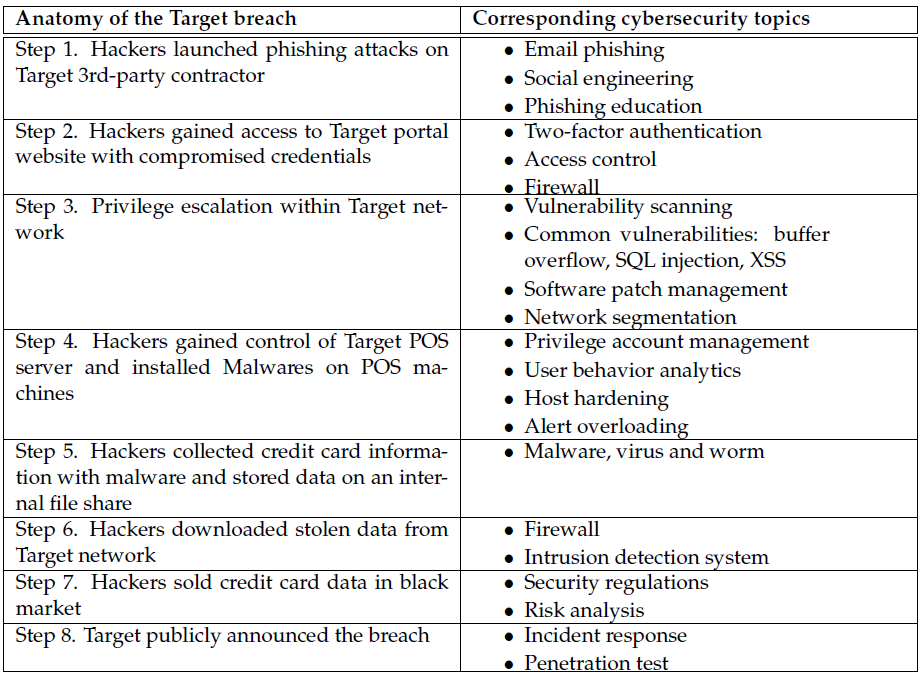


Figure 3: Analysis of the Target data breach

**Cybersecurity topics:**General topic: Email phishing, Malware, Access control, Firewall.  
  
**Teaching resources for the case:**A study package with the following materials was developed for the Target case:  
a) A PowerPoint presentation explaining technical details and lessons learned for the case: used by the instructor to guide the classroom discussion.   
b) A list of discussion questions: It is suggested to ask students to finish the discussion questions before attending the in-class discussion.  
c) A video tutorial introducing the case: For instructors or online students.   
The video can also be used before the in-class discussion. Students will be asked to finish the video before attending the in-class discussion.

**Additional third-party resources for the case:**[1] US Senate Report. A kill chain analysis of the 2013 target data breach, 2014.  
[2] Michael Kassner. Anatomy of the target data breach,2015. Available at http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.  
[3] KrebsonSecurity. Verizon security report on target, 2015. Available at https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.  
[4] Cyphort. Dissecting the target breach, 2014. Available at https://www.youtube.com/watch?v=hiKoBxn3smY.  
[5] Cyphort. Malware’s most wanted backoff pos malware, 2014. Available at  
https://www.youtube.com/watch?v=VRsDssFfzzU.  
[6] Web Privacy Wiki. Target data breach, 2016. Available at http://web-privacy.wikia.com/wiki/Target\_Data\_Breach.  
[7] Alert Logic. The Target Data Breach: Anatomy of an Attack. Available at https://www.youtube.com/watch?v=ap8RAjXO1C8.  
  
**Language:**English

**Date created:**   
May 1, 2023

**Last update:**   
May 1, 2024