Jasmyn Wilhelm 24 October 2024

CYSE 280 - Windows Systems Management and Security
Professor Malik A. Gladden
Homework 8

Short Answer Questions (short answers should generally be at least three to four sentences in length. However, it is important to be as concise as possible when responding.) or you may choose to **Upload a Two-Minute Audio or Video recording** to answer the following questions.

Listen to "Episode #6: Beirut Bank Job of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/6/

Based on the podcast, answer the following questions.

1) What is Jason E. Street's approach to performing security awareness engagements, and what is the ultimate goal of these engagements?

Jason's role in the security awareness engagements (SAEs) was to test whether breaches were possible. He describes them as a form of teaching rather than a red team engagement. He often does not go into the SAEs with a plan and often has a "YOLO" approach. In the podcast, Jason states, "We win by informing and giving knowledge to others. You may not know what the threats are."

2) How did Jason successfully gain access to multiple computers at the first bank branch in Beirut? What was his strategy?

Jason was challenged to compromise the bank's networks after Jason went downstairs and showed a sneak peek of how he could compromise their branch. He went into the bank with his normal disguised equipment as he did not have a plan and just played onto actual events. The first step was confidence acting like he belonged at the bank and walking to the executive office. After seeming to come out of the manager's office, the executive hardly questioned Jason, allowing him to insert his rubber ducky USB into her computer. The USB does not infect the system as he mentioned he is not doing a red team exercise. Instead, it opens a text box and allows him to type 'Hello' just to prove a point. After this, he went to a teller machine and told the executive to complete an audit using the same excuse and within 15 minutes he had completed his task. He used this ruse many times and was able to leave the building 3 times with stuff and was never caught. Eventually, Jason waited for the bank to close to inform the staff what had occurred and informed them of the dangers.

3) **What mistake did Jason make that led to him being discovered at the wrong bank? How did he handle the situation?**

Jason has a loving relationship with Diet Pepsi, resulting in him needing to desperately use the bathroom on the way to the bank. Due to most bathrooms being on the second floor in Europe, when Jason went upstairs used the bathroom, and began working immediately after. He used his fake Microsoft badge to get someone to allow him to inset his USB drive. He then moved on to the second and third computer before being approached questioning his intentions and qualifications. He was questioned and then impulsively stuck his USB into the wrong bank executive's computer to ‘prove his innocence’ and that it was ‘harmless’. That did not play over well for Jason; luckily, the person who hired Jason found him after realizing he had gone for a long time. After some time and Jason’s nervousness growing the situation did get resolved and Jason educated the wrong bank’s team about their response such as how to improve and mistakes made.

4) **What lessons did Jason emphasize to bank employees at the end of his engagements, and how can organizations improve their physical and digital security based on his experiences?**

Jason stresses the value of exercising caution and skepticism before entering a building. He cautions about phony messages and encourages individuals to double-check new relationships. Additionally, he suggests double-checking with the sender and confirming the identity of strangers. He stresses the value of being firm and kind, as well as not allowing someone to enter with your badge and ID. This is a vital part of preserving security and is a security policy rather than a personal choice.

References:

The Beirut Bank job – Darknet diaries. (n.d.). https://darknetdiaries.com/episode/6/