Jasmyn Wilhelm 21 November 2024

CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 11

Listen to “Episode #36: Jeremy from Marketing of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/36/

Based on the podcast, answer the following questions.

1. **What were some of the challenges Jeremy encountered during this penetration testing and social engineering process?**

   Selecting what tools to bring to the penetration test was Jeremy’s first challenge. Although he wanted to be prepared for carrying out the penetration test, he did not want to make his client's staff feel suspicious. Jeremy also had to use a low-level employee account with very limited access to breach his client's network as part of the penetration testing process. The last difficulty Jeremy faced was winning over the staff members of his client company.

2. **What were some of the technical techniques that Jeremy from Marketing used to manipulate the company’s network?**

   The process for gathering data about a network, including hosts, linked devices, usernames, group information, and other relevant information, is known as network enumeration. Network enumeration was Jeremy's first method to change the client's network. The second method that Jeremy used to control the client's network was using the Wireshark tool to analyze network traffic. To register a fake employee account and connect to the client organization's network, Jeremy adopted MAC address spoofing as his third method of network manipulation.

3. **What were some of the social engineering techniques Jeremy used on the company and its employees?**

   Jeremy tried three social engineering approaches to get into the client organization's office. He grabbed water, walked to the bathroom, and went around to make himself noticeable. He met staff members and opened discussions randomly to gain their trust. He persuaded Jane from the accounting department to give him her MFA (multi-factor authentication) code by acting as someone from leadership.

4. **How did the company respond to the attack and what measures did they take to prevent similar attacks in the future?**

When the client company saw that Jeremy was using Microsoft PowerShell on a finance employee's computer to imitate an attack. Jeremy took part in a discussion with the company's chief information security officer after the attack was sucessful. In order to defend the network against further attacks, the CISO used this information to find vulnerabilities and place tighter security measures in place.

5. **What lessons can we learn from the story of Jeremy from Marketing about the importance of cybersecurity training and awareness for employees?**

This story shows how easy victims are to online dangers, how important it is to be alert to phishing scams, and how regular education and fake attacks are needed. The incident also shows how crucial cybersecurity is to be included in businesses and that training be consistent rather than random. Creating clear procedures for suspicious activities is also important since informing staff members on how to report these issues can help the company respond quickly and minimize damage. Overall, all organizational levels should place a high priority on cybersecurity.

Resources

Jeremy from Marketing – Darknet Diaries. (n.d.). https://darknetdiaries.com/episode/36/