Darknet Diaries, Episode # 36: Jeremy from Marketing

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

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

July 10, 2025

Short Answer Questions: Short answers should typically be three to four sentences long. It is crucial to be concise while providing a thorough response. Alternatively, you have the option to upload a two-minute audio or video recording to answer the questions.

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?

Jeremy (the pen-tester known as Tinker) faced multiple challenges. First, he could only bring minimal gear to the building site to avoid suspicion while still being effective. He relied on his rogue laptop and heavily equipped small devices, such as USB sticks. Second, he operated with limited initial access to the network as a new marketing employee (i.e., a low-privilege account), which restricted his ability to move laterally within the network and forced him to escalate within tight constraints. That included evading antivirus detection, avoiding endpoint detection and response (EDR) solutions, and staying off the radar of the IT team.

Third, he encountered unexpected technical defenses that hindered his progress, such as close monitoring software and restrictive local administrator rules and policies. He had to closely monitor his behavior and apply specific pen-testing practices at particular times of the day so that it would not be flagged and send notifications or alerts to the IT department. Fourth, the social engineering and psychological preparation aspects were challenging because of the constant need to maintain a credible persona ("Jeremy from Marketing") while probing and manipulating others for information without raising suspicion.

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

He began with internal network enumeration using standard PowerShell and Windows commands (i.e., net user, net group) to discover domain users and servers while remaining anomalous. Jeremy used Wireshark on his rogue laptop to passively capture broadcast traffic, identifying hostnames and devices in the subnet. He also used Sysmon (a Windows Sysinternals tool) to monitor logs sent to a SIEM (Security Information and Event Management) system for reconnaissance. Lastly, he deployed Responder, a tool to spoof network services and capture credentials which enabled him to authenticate as another colleague user. These methods allowed him to test vulnerabilities and attempt to escalate privileges, though the company's monitoring thwarted some efforts.

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

Jeremy used pretexting while posing as a new marketing hire to gain trust from other company employees and unauthorized network access areas, using his role to ask seemingly innocent questions to extract useful information. He focused on blending into the workplace environment, leveraging a curious persona in social interactions to find security weaknesses without overt confrontation. For example, he would casually stroll around to appear innocuous and gain familiarity, engaging staff in small talk while grabbing water in the break room to lower guards and subtly glean information. Lastly, he attempted to elicit MFA codes from employees through friendly conversation and installing malware via USB sticks in other events, impersonating or pretending to be in a position of authority within the IT department.

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

The company responded by having an IT team member physically monitor Jeremy, indicating active surveillance. The company utilized activity monitoring tools, including Sysmon and a SIEM, to identify unusual behavior. Jeremy’s use of PowerShell from an unusual (Finance) department triggered alerts, too. After the engagement, the CISO debriefed Jeremy to understand the vulnerabilities exploited and then strengthened security controls, including tightening privilege levels, enhancing logging and alerting, and reinforcing cybersecurity training and awareness programs to prepare employees for insider threats better.

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

First, physical and social access are major attack vectors and can become major vulnerabilities—anyone who “looks the part” but has not been vetted can exploit human trust. Second, the episode highlights the value of in-depth network monitoring and incident response, as real-time detection and alerts helped prevent major damage and unauthorized access (internal and external) from occurring. Second, there is a need for employees to recognize and identify unusual behavior and social engineering tactics, as Jeremy's cover relied on exploiting employees' and colleagues' trust. Lastly, companies must emphasize and implement ongoing security training to identify MFA handling, verify unusual requests (even from insiders), and the value of monitoring tools to detect technical anomalies.