Darknet Diaries, Episode # 77: Alberto

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

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

June 26, 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 #25: Alberto of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/25Links to an external site.
Based on the podcast, answer the following questions.

1. What motivated Alberto to become a hacker?

Alberto had an intense curiosity and a desire to explore the limits of computer systems and their source code. Growing up in the early Internet era, he was fascinated by the challenge of breaking into different network systems and gaining unauthorized access. He viewed hacking as solving puzzles: poking around to find system vulnerabilities, then later reporting them to the network administrators or companies so that they could fix and improve them. His involvement in online hacking communities continued to fuel his interest in penetration testing and ethical hacking as he sought additional education, job promotions, financial gain, and recognition and respect among his peers.

2. What were some of the major hacks or cybercrimes that Alberto was involved in?

While he primarily conducted security audits and responsibly disclosed vulnerabilities, his most notable offenses occurred in 2015 and 2017. Alberto discovered an admin/admin login on a Uruguayan medical provider's site and allegedly accessed and exfiltrated medical records like his girlfriend's health information. He could not believe how easy it was to hack the medical provider's database. He understood the gravity of the situation, so he took the findings and notified the proper government and company authorities. Soon after, the IT professionals from the medical provider informed him that they had immediately resolved the system vulnerabilities.

Two years later, in February 2017, the same medical provider facility was hacked, and patient records were stolen. The attacker sent a threatening email to the medical provider demanding they pay an amount in Bitcoin to them (15 BTC in total) or the attacker would release the patient data to the public; what was odd is the email provided no method of or destination name for transferring the funds to the attacker, making the threat look out of place and not the primary goal of the attacker. After months of investigation and debilitation, it remained unclear exactly how and why the person exfiltrated the information.

3. What were some of the biggest risks and rewards of being a hacker, according to Alberto?

Rewards include the thrill of discovery, intellectual challenge, and respect within cybersecurity circles. However, the **risks** are severe: legal consequences, arrest, potential prison time, and reputational damage. In Alberto's case, crossing the line—whether intentionally or not—led to him becoming Uruguay's first hacker imprisoned, illustrating that curiosity can carry a high cost, regardless of whether one has good or evil intent to improve systems and enhance people's lives.

4. How did Alberto eventually get caught and what were the legal consequences he faced?

After seven months since the incident, Alberto was one of two people accused of the hacking event. The authorities claimed they traced back the attacker's IP address to Alberto's primary residence. Investigators traced the hack through logs and found extensive evidence at his home: over a dozen hard drives, tools, blank credit cards, hardware Bitcoin wallets, and an Anonymous mask. The police thought that if he had such an enormous "treasure-trove" of hacker paraphernalia, he had to have been the hacker. Alberto attempted to reason with the police, stating that he was using the hacking tools and technology for educational purposes, including writing papers and serving company clients. Later, he admitted to sending the extortion email in fear of the police questioning and imprisoning his girlfriend and mother. The police charged him with extortion and unauthorized access to confidential information, convicted, and sentenced to serve time in a high-security prison—making him Uruguay's first incarcerated hacker. The police detained him for a total of nine months.

5. What lessons can we learn from Alberto's story about the dangers of cybercrime and the importance of cybersecurity?

Alberto's experience highlights that even well-intentioned hacking—or ethical hacking conducted without proper authorization—can lead to serious legal backlash. It highlights:

- There is a critical need for proper authorization and responsible disclosure programs.
- Institutions must secure basic configurations, such as default credentials.
- A lack of cybersecurity understanding in the legal system can result in harsh or unjust outcomes.

Ultimately, the story highlights the significance of clear legal frameworks for cybersecurity and the dangers of exceeding legal boundaries.