Clarence V Kimbrell Jr
March 30, 2023

CYSE 280 – Windows Systems Management and Security

Professor Malik A. Gladden

Homework 11

1. What were the motivations behind the attack and who was responsible for it?

After a lengthy search, the FBI determined that a person by the name of Yevgeniy Nikulin was responsible for the hacks on the three major websites LinkedIn, Dropbox, and Formspring.

2. How did LinkedIn respond to the breach, and what measures did it take to prevent similar incidents from occurring in the future?

LinkedIn responded very quickly after they found out that their database was breached. Three things were done after the attack which was forcing employees to change their passwords. Then they created a new engineer account for the person who initially got hacked. After that, they rebuilt servers to make sure no traces were left on the systems.

3. What were the specific vulnerabilities that the attackers exploited to gain access to LinkedIn's database?

The hacker found out that one of the admins had remote access to LinkedIn’s database. This became the staging ground for the attack. The employee was hosting small websites from his house which led the hackers to gain more access to their computer. This eventually led to gaining access to LinkedIn’s information which they used to steal data.

4. What were some of the challenges in investigating and attributing the LinkedIn Incident to identifying the responsible group or individual?

One of the challenges that made this investigation difficult was all the information found could be traced back to a different county. This made it difficult to get information quickly which led to complications.

5. What lessons can be learned from this incident about the importance of strong password hygiene, and how can individuals and organizations better protect themselves against cyber-attacks?

The biggest lesson to be learned from this incident is to always salt your hashes. This provides an additional layer of protection to password hashes. Then another lesson that can be learned is

these companies were not using anomaly detection. Which allowed anyone to just use a VPN to gain access anywhere in the world.