Jasmyn Wilhelm 31 October 2024

CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 9

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 #29: Stuxnet of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/29/

Based on the podcast, answer the following questions.

1. **What was the intended target of the Stuxnet attack, and why was it deemed a high-value target?**

The attack against Stuxnet was designed to target Iran. The US considered Iran a high-value target because of its ties to Pakistani nuclear weapons traffickers. Iran possessed its own uranium enrichment facilities, which the US later learned might be used to create nuclear weapons.

2. **Who is believed to have created and launched the Stuxnet attack, and what motivated them to do so?**

The United States and its ally, Israel, combined to build Stuxnet. Both the NSA and the CIA provided USB drives to Iranian employees at the nuclear plant in order to physically install the drives onto the offline computer network, which is how Stuxnet was started. Iran is a geographic rival of both the US and Israel, and both countries sought to stop Iran from developing nuclear weapons, which is why they launched Stuxnet.

3. **How was Stuxnet able to evade detection for such a prolonged period, and what led to its eventual discovery?**

By using a fake digitally signed certificate, Stuxnet managed to avoid discovery by tricking Iranian computers into letting the code execute on the computer network of the nuclear building. In addition, the Stuxnet virus managed to avoid detection by taking advantage of software flaws in the nuclear centrifuges that allowed the US government to raise the centrifuges' operating speeds, which ultimately led to their failure, without the software of the centrifuges noticing. Stuxnet was found because it invaded external Iranian computer networks in addition to its main target.

4. **Which two U.S. government labs were utilized, and what specific activities occurred at each facility?**

The Oak Ridge facility in Tennessee and the Idaho National facility were the two US government laboratories that were involved. Many ways to damage the centrifuges of the Iranian nuclear site were developed at the Oak Ridge lab. The Oak Ridge Lab's attack techniques were tested in a realistic environment at the Idaho National Lab, which also provided information on Iran's nuclear facility.

5. **Which two U.S. Presidents were involved in the Stuxnet attack, and what were their respective roles in the process?**

George W. Bush and Barack Obama were the two US presidents who participated in the Stuxnet attack. George W. Bush authorized the US government to continue Stuxnet's research and testing. Barack Obama spread the virus in 2009 and responded to the public's discovery of Stuxnet in 2010.

References

Stuxnet – Darknet diaries. (n.d.). https://darknetdiaries.com/transcript/29/