Your Name

Instructor Name

Date

Cyber Attack on HBGary Federal

**Question 1 Part A**

A content management system was created by HBGary’s website (Olson 2) . The CMS has several vulnerabilities and attackers were able to exploit these vulnerabilities. Anonymous attackers were able to gain entry by using new passwords that were updated by the employees.

**Question 1 Part B**

The attackers were able to exploit local vulnerability because the passwords that employees were using were not strongly encrypted.

**Question 1 Part C**

The attackers were able to use the social engineering of a network administrator. After hacking it, they were able to access the rootkit.com webserver.

 **Question 2**

The attack on HBGary Federal can be characterized as opportunistic. This is because it was the organization’s fault. They should have considered all security options by catering to the vulnerabilities of a new content management system. Also, they must have trained the employees to use strongly encrypted passwords.

**Question 3 Part A**

In any organization, employee data is always protected and is highly confidential. Hackers were able to retrieve not only the email addresses of employees but were able to retrieve usernames and passwords of the administrators for HB Gary Federal web servers as well. As hackers were able to access all the organization's data, they could have exposed confidential emails to the public which could cause HBGary Federal to lose lots of money and reputation.

 **Question 3 Part B**

The anonymous hackers hacked into HBGary’s website and after gaining access, they replaced it with a message indicating that they would release all the findings that Barr investigation had been doing on them. This activity can be described as an integrity attack as hackers not only gained access to the website but were able to corrupt the data and rewrote them.

**Question 3 Part C**

Anonymous took control of the organization’s emails while also erasing 68,000 emails from the system. This activity can be considered as an availability attack.

**Question 4 Part A**

Gaining access to Linux computers with the help of social engineering, hackers were able to access web servers and Barr’s Twitter account as well.

**Question 4 Part B**

Action G was done first because after gaining access to the rootkit.com webservers, hackers were able to access all the data of an organization.

 **Question 4 Part C**

Hackers need to gain access to the webservers to delete emails and other important data so action D was done first.

**Works Cited**

Olson, Parmy. “Anonymous Takes Revenge On Security Firm For Trying To Sell Supporters’ Details To FBI.” *Forbes*, https://www.forbes.com/sites/parmyolson/2011/02/06/anonymous-takes-revenge-on-security-firm-for-trying-to-sell-supporters-details-to-fbi/. Accessed 18 Oct. 2019.