Student Worksheet for Assessment

Students: *This worksheet is provided as a template. You are not required to use this document, but your response must include the same section headings (Executive Summary, Detailed Summary, etc.).*

Instructions:

Read the following article about the historical incident: the 2013 Target Breach. https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

You may need to conduct additional research on the internet to complete this assignment.

Write an incident report summarizing the incident in the article. Use the worksheet below to complete each section of your report.

1.	**Executive summary**. Provide a high-level explanation of the events of the incident. It should be no more than 2-3 sentences explaining what happened in the breach.
	Student Answer The company Fazio mechanical a HVAC company who is a vendor of target. The vendor was apart of a phishing attack that lead the attackers to be able to get access of credit and debit cards of customers of Target. Fazio employees used citadel to get access to fazio mechanical's login credentials.

2.	**Detailed summary of the incident**. This should include provided timelines and outside resources that may have been involved in the response. This section should be 200-300 words long.
	Student Answer The company target was attacked on November 27, 2013, which is Black Friday the busiest shopping day of the year. It was until nearly two weeks later the department of justice was notified. As of December 15, the company target hired a 3rd party forensic team to have the attack on the company mitigated. This attack started at the company Fazio mechanical who is a 3rd party vendor that did work on the HVAC system for Target. The attackers were able to get into Fazio systems through a

	phishing attack which installed Citadel which is a banking trojan. Once the trojan was installed they were able to gain access to Fazio login credentials. Its also noted that the company Fazio only had the free version of anti-malware that doesn't offer real time protection. Once the attackers had the credentials of the company, they were able to gain access to targets internal systems. It is most likely that target used active directory which led the attackers to gain access to targets internal system. Once in targets system the attackers used the malware code named trojan.POSRAM to attack targets (POS) point of sale. This trojan was able to gain customers credit and debit card information in real time. Once they have the customers information they were able to send that information to a remote server.

3.	**Major findings** of the incident as discussed in the article. This includes discussion on what contributed to the breach and indicators of compromise. Provide 2-3 bullet points summarizing your findings from the article.
	Student Answer -the company fazio not having a higher-level anti malware one that does offer real time scanning -Active directory still being accessible to 3rd party vendors once the work is completed

4.	**Recommendations for remediation**. Provide 2-3 recommendations discussing what the organization can do to prevent future breaches.
	Student Answer -once a vendor work is completely revoke credentials -having updated anti malware that offers real time scanning -adding a firewall between pos and any other internal systems on the network

5.	**Conclusion**. Discuss areas of the report you felt did not provide enough information about the incident and identify information missing from the report that would be helpful to an incident responder. Conclude with a brief summary that includes an explanation of why the event is important to study as a cybersecurity professional.

	Student Answer The thing that was not explained fully is how the attackers gained access to targets system with the 3rd party credentials. Its only assumed that they used different techniques. the hacking techniques that were used could be a teachable moment for the community to help future incidents to be prevented,