Assignment 5

by Nikhil T M

Submission date: 16-Oct-2021 01:39PM (UTC+0530)
Submission ID: 1675381911
File name: PES1UG20CS821.pdf (143.6K)
Word count: 774
Character count: 3594

Assignment 5

Name:Nikhil T M
SRN:PES1UG20CS821
Section:F

1. How well did the iPremier Company perform during the seventy-five minute attack? If you were Bob Turley, what might you have done differently during the attack?

Ans The whole organization responded really bad during the attack time and they didn't had any emergency procedures that need to executed or followed after the attack.after the attack also we can see that the none of the employees had any idea about this or as they haven't experienced such time of thing before so they haven't had any updated procedure to follow and as all were kept calling and none of them have an idea or a well detailed procedure to solve it. If I was Bob Turkey as soon as I was appointed I will ask for the IR plan and review it. If it was not up-to mark I would have updated it with detailed procedure and spread an awareness andtrain all the employee about the different types of attack . I will check leon and Joanne are up to the mark and doing their work properly by using the latest security and the proper utilisation of the organization resources by providing two step verification to all the employees and also if required I would have liked to add another team with experts which can be used to identify the attack and defend it I like to follow the principle during the attack like not to panic and disconnect the connection and responded in proper way I like to make another backup plan such that in these type of attack I could have responded it quickly through remote system and fix it as soon as possible .

2. The iPremier Company CEO, Jack Samuelson, had already expressed to Bob Turley his concern that the company might eventually suffer from a "deficit in operating procedures."

Ans The Jack Samuel have said to Bob Turley based on the regards of company's policies that the operating procedures are not up to date. It was clear that the operating procedures deficiency is the main weak point which caused a poor response to the attack. The employee didn't even knowhow to respond a DDoS attack. The company should have had a contingency plan which most standards IT companies have a If a solid IR Plan would have been in place the CEO Jack Samuelson would have taken it seriously and appropriate action would have taken.

3. Were the company's operating procedures deficient in responding to this attack? What additional procedures might have been in place to better handle the attack?

Ans According to my point of view Yes The company is having a failure in their operating procedures and It is clear based on how the company responded during their attack . as The company not had any of the emergency procedures which clearly shows the company have an deficit in operating procedures as none of them in their

company staff was known to these critical procedure and it was not updated also and the employees were not trained to how to respond to the attack in specific way. The organization was not to date by using the backup storage for keep track of the access log of the employee and find the cause of the attack quickly which results in further stop of the attacks if it have done there would been beneficial in handling the attack.
if the company had an adequate software like firewall etc then it would have easily dealed with such things like Dos attacks and a firewall may have helped to their standards, though the organization failed to defend the attack because of outdated procedure and unawareness of the employee.

4. Now that the attack has ended, what can the iPremier Company do to prepare for another such attack?

Ans After the attack is ended. the iPremier company should update their policies and procedural that need to followed and increase in the security such as updating the firewall and should focus on prevention and spread awareness about it and perfect detailed plan should be designed and all the assets are need to be backed up and monitored frequently should increase and keep the security up to date and provide extra authentication and identification on the employees. They can also buy additional devises and storage to keep track of log and implement biometric for identifications and authentications.

5. In the aftermath of the attack, what would you be worried about? What actions would you recommend?

Ans Once the attack is over I would like to analyze it clearly as much as possible in every stages so that I can get most of all the information from internal network or application system logs etc.Some of the questions need to be examined are

- Does it affect the assets ?
- Does it affect the whole network or specific server ?
- If attacked on specific services will it going to affect the other services also?
- What were the attack characteristics?
- What was the maximum network traffic reached?
- Which layer did the attack impact?
- Can we do anything with the digital foot print?
- Is any data altered ?
- Any changes in the log files?
- Is there further files like malware added to infect the systems?
- What type of pattern and protocols were used to perform the attack?

Assignment 5

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		