PES2UG20CS209_CaseStudy_iPremier

by Naman Choudhary

Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

Local DNS Attack Lab

Assignment – iPremier case study

1. The company might have handled the attack far better and did not handle it in a professional manner. The company and the data hosting service were not in contact. The software and protocols used to defend against these threats weren't properly optimised and maintained. The business prioritised the client's experience and responsiveness over security and robustness, leaving the website open to several threats and weaknesses. The employees of the company were not trained in case of an emergency like an attack. Things seem worse when we realise that there was no Disaster Recovery Plan(DRP) available to be referred to.

I as Bob Turley, I would have not waited around for Joanne to reach all the way to the data centre, and rather, would have contacted the web hosting service to save all the logs and then immediately for them to shut the website down till things were figured all out. Risking the website to run for longer could further risk compromising sensitive information like credit card details which were stored on the servers. I would then report the incident to a trusted cyber expert, who could take a look at the damage done.

2. The company's procedures of operation were indeed deficient in responding to the attack on its website. This is unacceptable for a company with such a high reputation and name in the market (which gave hope to many people with its exponential growth in the stock market). This meant that an attack on the company's website was waiting to happen, and the only question that remained was when. This in turn led to many other problems like being completely unaware and unprepared when the actual attack happen, which obviously was handled very badly. Also, the data centre company

service that they were using (QData) was not equipped with countermeasures for the attack.

The additional procedures that could be in place to handle the attack better are to include and enforce a highly experienced and skilful tech department, which would have helped evade the attack. Enforcement of an Incident Response Plan or a Disaster Recovery Plan(DRP) was necessary, which should have been the top priority by Bob Turley.

3. To prepare for any future attacks, IRP and DRP need to be implemented and the employees must be trained as soon as possible. The Business Continuity Plan should be updated and made up to today's standards according to Joanne Ripley, leader of the technical operations team. The new technical team should also be well-trained to be able to defend and provide extra security against any attacks in the future. The company should also force to shift to data centres inside or near the company headquarters, as well as, make sure it's in-house and is not using any external data centre service. The shift of the company ideologies should be more towards customer data and privacy. Strick measures should be taken to ensure these steps are implemented correctly. Help from a cyber security company can also be taken to make the work easier and faster to implement.

4. In the aftermath of the attack, is that eventually after the news gets out to the public and spread around like wildfire, the company stocks will take a big hit, which will devalue the company a lot. This will also cause a snowball effect, wherein, the customers will lose trust in the company, and finally, even resulting in lowering of sales for the company. It will take a lot of effort and time to regain the trust of the customers and value of the company back.

The company could also be criticised for being part of a data breach and exposing customers' valuable information. The iPremier file (B) contains a list of the actions that Joanne Ripley suggests the company take, some of which are indicated as steps. I'd advise that thorough logging is necessary and must be included. There must always be a cyber security task force. The need for effective communication between the company and the data centres also suggests that QData may not be the best option for the company. I would advise the business to temporarily shut down the website so they can reconfigure their data systems, pass it off as routine maintenance, and patch their vulnerabilities. The company should also make sure that they do not store credit card information on their web servers as this could be problematic from a legal point of view and should be handled properly and this should be highly discouraged in any workforce
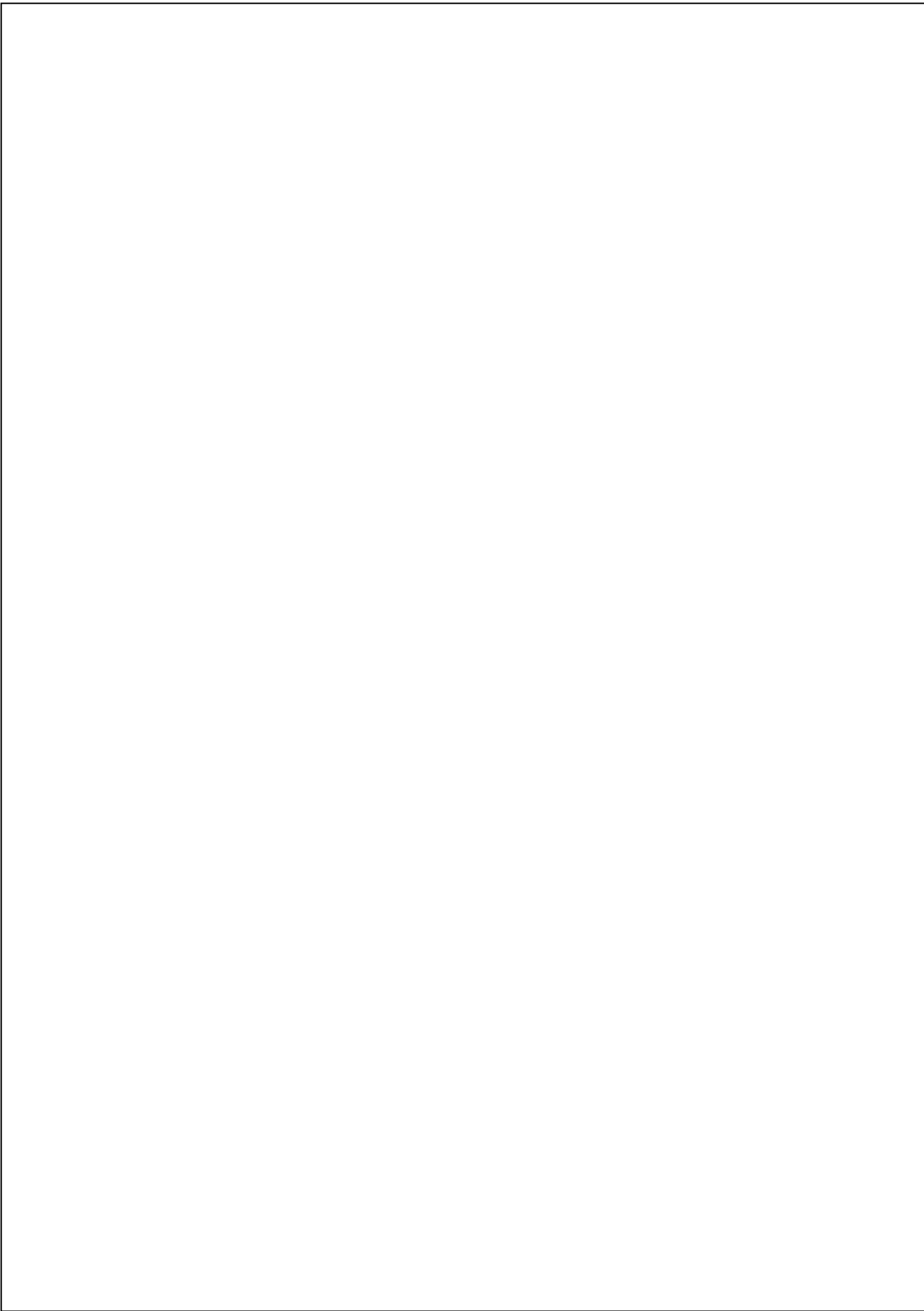
PES2UG20CS209_CaseStudy_iPremier

0%
SIMILARITY INDEX

0%
INTERNET SOURCES

0%
PUBLICATIONS

0%
STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		