**Assignment Sheet 2 (P 2.2)**

**The massive Panama Papers data leak explained (Panama Papers: “It was an email server attack”)**

“The email hack includes 2.6TB of data, including 4.8 million email messages and 2.2 million PDFs”

A data breach at Panamanian law firm Mossack Fonseca is being touted as the largest ever, at least in terms of the sheer volume of information leaked.

The leaked information allegedly details the ways dozens of high-ranking politicians, their relatives or close associates in more than 40 countries, including the U.K., France, Russia, China, and India, have used offshore companies to hide income and avoid paying taxes.

**The numbers:** The leaks reportedly cover 11.5 million confidential documents dating from the 1970s through late 2015. The 2.6 terabytes of leaked data include 4.8 million emails, 3 million database format files, 2.2 million PDFs, 1.1 million images, and 320,000 text documents.

**How did the leak happen?** Details are sketchy, but a representative of Mossack Fonseca has confirmed news reports saying the leak stems from an email hack. It's unclear how the email attack happened, but tests run by outside security researchers suggest Mossack Fonseca did not encrypt its emails with Transport Layer Security protocols.

An email server attack could have happened in "multiple ways," said Zak Maples, a senior security consultant at MWR InfoSecurity, a cybersecurity consultancy. It appears that the server itself was compromised instead of individual mailboxes brute-force in password-guessing attacks, because of the volume of data compromised, he said by email.

**"**This breach is quite possibly a broader compromise of the organization," Maples added. "Attackers may have compromised the Mossack Fonseca network and elevated privileges to that of a domain administrator or email administrator and used these elevated privileges to access and download all the data contained on the e-mail server.**"**

**What/who is/was affected? What/who is/was affected?**

High-ranked politicians, Celebrities including the U.K., France, Russia, China, Pakistan and India, have used offshore companies to hide income and avoid paying taxes. Their reputation is affected in worldwide and country image is also affected in somehow because these people are considered the ambassador of their countries.

**Are you affected (if so, how did you react)?**

No.

**May the university be affected?**

**Anti-Semitic Cyber Attack Hits Universities across Germany**. Universities across German have been hit by a cyber-attack. Many colleges confirmed that their network printers and photo-copy machines had been spontaneously printing racist and anti-Semitic flyers, out of nowhere. According to reports the affected academic institution include Universities in Hamburg, **Bonn**, Münster, Lüneburg, Bremen, Tübingen und Erlangen-Nürnberg. Meanwhile, the security breach has reportedly been closed.

**Which sources of information have you chosen and what do you think about the quality of the sources?**

We have chosen most links from very reliable resources and most people know panama papers are being well known issue around the world and its links almost very reliable and the information sources are much authenticated.

<http://www.computerworld.com/article/3052218/security/the-massive-panama-papers-data-leak-explained.html>

<https://nakedsecurity.sophos.com/2016/04/05/panama-papers-it-was-an-email-server-attack/>

<http://legalinsurrection.com/2016/04/anti-semitic-cyber-attack-hits-universities-across-germany>

<http://www.breitbart.com/london/2016/04/22/german-university-printers-flooded-anti-semitic-messages/>

**Second Solution**

**Assignment Sheet 2 (P 2.2)**

**Briefly Description about attack**

**Talk Talk (UK Popular telecommunication, internet provider & Paid TV Services Provider). Attack**

Last year October 2015 we have seen one of the UK’s biggest hacks that dominated news headlines in the British media. The mobile phone provider was the target of a bunch of teenage hackers who stole the details of over 20,000 customers. Talk Talk (Telecommunication Company) released an official statement that we are the victim of a “**significant and sustained**” cyber-attack, stating that its 4m customer’s personal information such as names, credit card and bank details may have been stolen.

**Who did it?**

In a message posted to code-sharing website Pastebin, a group claiming to be behind the attack shared some of the data it said it had appropriated. In these messages lie customer records that display names, emails and also passwords. One particular file suggests that when some users changed their password via the TalkTalk website, the new value was stored in plaintext -- meaning it may not have been secured in any way. TalkTalk admits on its website that "not all of the data was encrypted," and that appears to cover sensitive data like passwords and possibly even credit card and bank details.

Normally, secure websites will salt and hash sensitive user information. Instead of storing a password like 'QWERTY,' they'll generate a representation of it instead. This is either a long random number or a string of unique letters and numbers. When a user logs into a website that utilizes hashes, the system will take their password, convert it into a hash and then match it to the hashed value stored in the database. It means that if records are then stolen, information like passwords aren't immediately viewable. This method isn't 100 percent foolproof, though, as algorithms can still be cracked if an attacker has a lot of time and the right tools available to them.

**How was the data stolen?**

Looking at the unverified data dump, we ascertained that TalkTalk stored customer information in SQL databases. SQL is a very common online database structure and its popularity means that installations have become targets. Reports suggest that TalkTalk was subjected to a distributed denial-of-service (DDoS) attack that enabled the attackers to utilize SQL injection techniques. SQL injection allows an attacker to feed commands to a database (that shouldn't normally be accessible) via a poorly-designed website form or input box.

**What/who is/was affected? What/who is/was affected?**

Talk Talk (UK Popular telecommunication, internet provider & Paid TV Services Provider) their customer’s personal details, privacy and company reputation and also the business was affected.

**Are you affected (if so, how did you react)?**

No.

**May the university be affected?**

Universities across the UK have reported problems with their internet connections following a cyber-attack on the Janet computer network. It was a breaking news headline in UK biggest newspapers “**Janet down: Computer network at UK universities continues to face problems after DDoS cyber-attack**”.

Jisc, which operates the network on behalf of UK higher education providers, reported a distributed denial of service attack on 7 December 2015 and made progress towards stabilizing the system, but then reported a further series of attacks which continued into 8 December. Initially, the problems were reported to be affecting Janet users in the **Manchester** area, but it then became clear that the UK-wide network was affected.

Higher education institutions across the UK use the **Janet networ**k, which supports the .ac.uk and .gov.uk domains, as well as the **Eduroam Wi-Fi** network used at many universities.

**Which sources of information have you chosen and what do you think about the quality of the sources?**

I have chosen most links from very reliable resources like BBC and also read about these attacks on company official websites and seen some videos about them so I think that these given information could be reliable

<http://www.bbc.com/news/business-34743185>

<http://mancunion.com/2015/12/08/breaking-news-university-network-under-sustained-cyber-attack/>

<http://www.ft.com/cms/s/0/9bfb4e72-7965-11e5-a95a-27d368e1ddf7.html#axzz4808gUBPX>

<https://www.timeshighereducation.com/news/cyber-attack-janet-network-disrupts-university-internet-connections>

<http://www.engadget.com/2015/10/23/talktalk-hack-explainer/>

<http://www.information-age.com/technology/security/123460603/sql-injection-how-avoid-same-fate-talktalk>

<http://www.infosecurity-magazine.com/news/sql-injection-possible-vector-for/>

<http://www.information-age.com/technology/security/123460603/sql-injection-how-avoid-same-fate-talktalk>

<http://www.infosecurity-magazine.com/news/sql-injection-possible-vector-for/>