COMPUTER FORENSICS (INCS-712)

PROJECT SCENARIO EXAMPLE

Dunder-Mifflin Co is a paper supply chain in Canada with head office in Toronto. The CEO of this company is Creed Bratton, and the vice president is Janet Levinson. It has three other branches in Vancouver, Abbotsford, and Montreal. All branches have seven departments, namely; Sales, HR, quality analysis, accounting, customer service, IT and warehouse.

The Vancouver branch has 300 employees in total, and the Regional manager is Mike Scott who is a victim in this scenario. There are about 100 employees in the sales department at Vancouver Branch, one of them; name Dave Schrute is unhappy with the treatment he is getting from his Regional Manager and his salary as well. He decides to take revenge against his manager. Dave sends a phishing e-mail to Mike Scott (his manager) asking to change the password of his email account for security purposes. He uses social engineering tool kit available in Kali Linux to send the phishing email. This email has a Typo squatting link to a fake mirror of the Gmail website that records all the passwords. The manager takes the bate and tries to change his password, but he ends up revealing the password to Dave. After gaining access to Mike's private email account, Dave starts to look for sensitive information that he can leverage. He comes across an email conversation between Mike and vice president Janet, where he finds out they both are having an affair. Immediately after learning this information Dave sends an anonymous threat email to Mike asking for a hike in salary for 20 random employees, or he would forward the screenshots of those conversations to CEO. Dave selected 20 random employees which included him as well to maintain his anonymity.

Mike starts freaking out after receiving this email because he knows he will be in trouble if he hikes up 20 employees' salary or if his CEO gets to know about his affair. Mike, not knowing what to do tells Janet (Vice President) about the threat email. Mike and Jan discussed among each other and decided to admit their mistakes in front of the CEO and launch a company-wide investigation for the culprit behind the email threats.

Any questions please free to contact me via email: smuttabh@nyit.edu!!