Noah Berson & Loi Tran
MIS5211.007

Wells Fargo Executive Summary

Wells Fargo has been at the forefront of a huge accounting scandal in recent weeks. Wells Fargo has been exposed for creating over 2 million user accounts (savings, credit cards, checking, etc.) without their customer's consent in order to inflate market share prices. In light of these events, Wells Fargo customers, the US government and other legal entities are furious about the lack of oversight and accountability in the organization's structure and processes. Wells Fargo fired approximately 5,300 employees stating that lower level employees and management were to blame instead of company culture. A lack of oversight in financial processes can only make a customer wary about how Wells Fargo is protecting or not protecting their personal and financial data.

We have conducted a basic reconnaissance on the organization's cyber-security controls by accessing publicly available information to identify potential attack vectors that could be exploited. The reconnaissance consisted of DNS searches using the command line; NSlookup, Whois, nmap and dig; and ARIN and DNSLookup.com websites. Google hacking techniques were also used to enumerate Wells Fargo web portals, documents, and other resources. Temple's Foxnet, Wells Fargo's career page, Monster.com, and LinkedIn were used to identify the technologies that were being used at Wells Fargo. LinkedIn also provided insight to the type of personnel the company hires.

We started our reconnaissance with terminal command searches. The DNS searches provided and insight into the organization's headquarters, network resource IP ranges, physical location of datacenters, and administrator contact information. From DNSstuff.com, we were able to view IP addresses for Wells Fargo name servers and were provided a list of potential vulnerabilities that was flagged when traffic was requested from the servers. Attackers may use these warnings to exploit the Wells Fargo systems.

Job searches on public sites, including Wells Fargo internal career portal, showed us what types of programs and applications were being used at the company. Some of the programs mentioned were MS SQL Server, PL/SQL, Advent APX, RESTful and SOAP web services. A search on LinkedIn for Wells Fargo employees provided us with a list of Temple Alumni that could be used for social engineering attacks, particularly for attackers with a Temple background.

Google hacking techniques revealed a point of major concern for this reconnaissance exercise. We were able to access the company's Corporate Retirement portal by using "site:Wellsfargo.com inurl:admin." Further, by utilizing nslookup and nmap we were able to find the IP address and open ports for the server hosting the corporate retirement site, which was marked as a private system. We were also able to obtained a 229 page "Team Member Handbook" by using "site:wellsfargo.com teamworks," that provided the company's policies, procedures, and detailed information for additional resources for the employees. The sensitivity of the document is questionable due to its nature and may be used by competitors to learn of Wells Fargo practices.

Sources: http://www.nytimes.com/2016/09/21/business/dealbook/wells-fargo-ceo-john-stumpf-senate-testimony.html