Ahmed Alkaysi

9/18/16

Reconnaissance on SunGard

For the reconnaissance assignment, I chose to research the company SunGard, which is based out of Wayne, PA. SunGard is a company that primarily focuses on providing “mission-critical software and IT services to institutions in virtually every segment of the financial services industry.”**1** SunGard was recently acquired by Fidelity Information Services (FIS) which is the “world’s largest provider of core processing, card issuer and transaction processing services to financial institutions and businesses worldwide.” **2**

The tools used in this recon mission included: Netcraft, ARIN, Google Hacking, and some job posting boards. Using ARIN, I found a Point of Contact (PoC) for the domain SunGard.com. Through Netcraft, I was able to determine that BiGIP provided the tech for the Web Server, although the OS was unknown. Searching potential job openings did not produce any good results, as there were very few technical positions available. It seemed like the company was focused on hiring financial related positions such as: account manager, billing analyst, and compensation analyst. Eventually I focused on using Google hacking, which gave me the best results by far, as I found a treasure trove of information.

The deeper I dug using Google hacking, the more potential vulnerabilities were discovered. My strategy was to begin Google hacking by running a basic query using SunGard in the SITE command, and filtering out the common subdomains such as ‘support’ and ‘financialsystemsjobs’. I chose to do this to see if there were any uncommon sites with vulnerabilities using the lowest level of effort. Since there weren’t any results that satisfied me, I started to use more specific queries.

The next command I chose to use was INTEXT with the keyword ‘confidential’. I wanted to see if there were any sites or documents that were not meant to be seen by the public, and I succeeded. This query returned results with PDF files of instructions on how their fee system works, the email address of a client, possible account numbers, diagrams, and many other “confidential and propriety” info as stated in their docs.

After I saw multiple PDFs being returned, I tried looking for spreadsheets by using the FILETYPE command specifying ‘xlsx’. An excel document was returned containing data on everyone that registered for an event ran by SunGard. The information in this excel included the registered parties first and last name, the company they worked for, their email addresses, and their respective positions. A lot of damage can be done if this type of information gets in the wrong hands.

Another query I used included the ‘login’ keyword to see what kind of SunGard’s sites/products required login information. I found a site that was not secured by HTTPS requiring login to SunGard’s Wealth Management Resource Center. This is a security gap that could be taken advantage of by a man-in-the-middle attack.

In the end, I was very surprised at the amount of vulnerable information using Google hacking returned, especially for a company in the financial services industry. I did not expect to see such valuable information in “confidential and propriety” documents available on the internet. Although a lot of this information might not be healthful for a large scale cyberattack, this type of info can definitely be used for social engineering.