Kari Green & Sean Stockwell

Super Duper Sketchy Corp Pen Test

Overview

We are searching for vulnerabilities within the computer system at Super Duper Sketchy Corp (SDSC). We were able to break into the Wi-Fi network, perform social engineering to obtain passwords, and then break into the server where many more company assets were vulnerable.

Methodology

To break into the Wi-Fi network, we used aircrack to crack wireless passwords. We needed to create a potential password bank, which was incredible simple given the very few password options (a 3 character password doesn’t have very many permutations).

To obtain the password to the server, we sent a phishing email to the helpdesk using netcat. We then were able to access the server using this password. We were able to gain remote access to the server at this point, as the port number needed for this was in the Welcome.txt file.

On the server, within the tmp directory, some .pcap files were found. We copied these pcap files to our computer and analyzed the data to find admin password information. We then were able to use the admin password information to login to the admin section of the website where we found information on layoffs and the password to the executive lounge.

Findings

Wi-Fi Password: 9cy

TCP Port 47923 to access the server off of the wireless access point

Admin info: mattley - 388roxmysocks

Password to executive lounge: h4ppie8rthDay

Corporate secrets: 30% of the workforce will be laid off in March

Remediation