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 a port scan to identify the correct IP of the server, perform social engineering to obtain passwords. Once we broke into the server, we were able to capture network traffic and obtain passwords and then use the administrative password to gain corporate secrets from the website.

**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).

Once on the Wi-Fi, we did a port scan (nmap -p 25,22 192.168.0.0/24) to look for any open SSH ports (22) and open SMTP (25). We were able to find an open SSH port and an open SMTP port for the IP address 192.168.0.23.

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.

We snooped traffic on the server using tcpdump and created a .pcap file. In these packets, we were looking at GET admin requests in the HTTP protocol and were able to get the login in information of the admin and of another user. 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: EECS388-9cy
  + 192.168.0.23 SMTP Port 25 to access the mail server
  + 192.168.0.23 SSH Port 22 to access the server on the superdupersketchycorp wireless
  + 192.168.0.23 with TCP Port 47923 to access the server off of the wireless access point
  + Admin info: mattley - 388roxmysocks
  + Other user login: hewen – EkW8SXu
  + Password to executive lounge: h4ppie8rthDay
  + Corporate secrets: 30% of the workforce will be laid off in March

**Remediation**

The complexity for the wi-fi password should be upped. It’s incredibly easy to make a list of every possible password for a 3-character password limited to numbers and lowercase letters, however it’s nearly impossible to make a list of all 15 character passwords that contain upper/lower case letters and numbers (6215). The password could be made even better by including special characters. This will make using aircrack significantly more difficult, if not impossible.

To avoid the phishing attack where we stole the server password, we would recommend that when receiving an e-mail, you should probably respond to the address that sent it versus the reply-to field. Also, it is important to train your employees on how to identify phishing emails and to never click on links in emails or send passwords in plaintext over email.

We were able to identify the admin login by snooping the web traffic. To avoid being able to identify the admin login (or any other login used on the webpage), the HTTP login request information should be encrypted rather than plaintext.