Team: Team 3

Inject Number: 20

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 04 Mar 2017 17:23:49 +0000

From: Chief Information Security Officer

To: Infrastructure Team

Subject: 001 Basic Audit of IoT (Raspberry Pi)

Our Chief Information Officer read an article over the weekend that described the Mirai Botnet and how it exploited the Internet of Things (IoT) devices across the world to create a DDoS. The Botnet used basic network services and common accounts with no or simple passwords on IoT devices. Rather than disconnect our Asterix PBX from the network and take down our Voice over IP system, I convinced him that we could perform a quick audit to alleviate his concerns. Please provide in a business memo format the following details concerning our Raspberry Pi IoT device:

- Detailed version information on the OS that the Raspberry Pi is running
- A list of all accounts and groups on the system
- Whether the accounts have passwords enabled or are disabled/inaccessible if they do not have passwords
- A list of all ports the Raspberry Pi is listening to, both udp and tcp
- A list of all the log files the device is capturing in /var/log (if they are elsewhere, please indicate where and what is logged)
- A snippet of the log showing one successful login via ssh

These should be easily obtained via the command line using standard Linux commands. If you have difficulty obtaining any of the items, please briefly explain in the memo so the CIO does not have follow-up actions on this request.

Thank you.

Chief Information Security Officer