Team: Team 3

Inject Number: 14

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 04 Mar 2017 16:27:59 +0000

From: CSO

To: Security/IT Admin Team

Subject: 001 Secure IoT Devices

Our Security Team has recieved alerts from FBI and other Security Organizations that have indicated that the threat level is very high for attacks agianst any rasberry PI devices being used please secure as best as possible using the following recommended procedures: (remember to use Sudo command to run commands as root user)

1. Secure the default admin and root accounts.

- add a new user account to be the new admin/root account.
- Either disable and Change the default Raspberry Pi user 'pi' password or
- Remove the default 'pi' user from your Raspberry Pi

(Especailly since this information is publically available to everyone on the internet.)

2. Perform and configure for Security Updates automatically on the Raspberry Pi

- sudo apt-get install unattended-upgrades

Type the following command to edit the configuration file for unateended-upgrades:

- sudo nano /etc/apt/apt.conf.d/50unattended-upgrades

The packages that we want to upgrade are located in between Unattended-Upgrade::Origins-Pattern { } in the configuration file.

You will either need to uncomment the Raspbian line or add the following line to perform only Raspbian Jessie Security updates:
"o=Raspbian,n=jessie,l=Raspbian-Security";

3. Setup SSH Key Pairing to Login to your Raspberry Pi (and require a passphrase)

SSH Keys allow you to login to your server without a password. The client and server will use these keys to authenticate the client which allows it access.
Adding a passphrase would go the extra step and really lock-down our server and making it virtually impossible to connect into without the SSH key and the passphrase.
if unsure here is a quick tutorial on how to setup SSH key pairing:
http://kamilslab.com/2016/12/17/how-to-set-up-ssh-keys-on-the-raspberry-pi/

4. Investigate the use of Install Fail2Ban to ban brute-force attempts on our Raspberry Pi

```
- sudo apt-get update
- sudo apt-get install fail2ban
```

edit our SSH Fail2Ban configurations. Open up the '/etc/fail2ban/jail.local' file with the following command:

```
- sudo nano /etc/fail2ban/jail.local
```

add the following settings:

```
[ssh]

enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
bantime = 900
banaction = iptables-allports
findtime = 900
maxretry = 3
```

After pasting the settings hit CTRL+X and then Y to save the configuration file.

Restart Fail2Ban with the following command to make your configuration settings live:

```
- sudo service fail2ban restart
```

Please submit memo style summary report with screenshots of each of the configuration settings that your team has applied to prove these settings have been configured for each step.

CSO

Thank you.

CSO