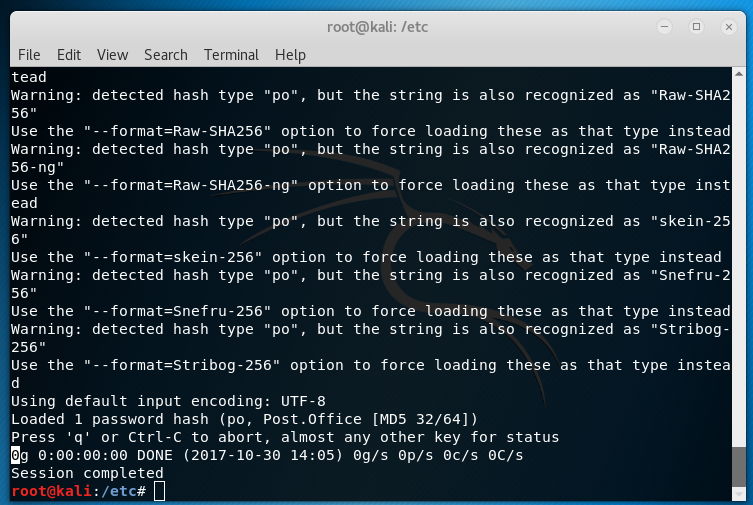
**Análisis de seguridad Dispositivo 1 : Control de Luces y Calefacción**

**Desencriptando archivo passwd de API WEBIOPI usando la herramienta Jhon the Ripper:**

Haciendo uso de la herramienta Jhon the Ripper la cual puede obtenerse desde el siguiente link (<http://www.openwall.com/john/>) se realiza el crack del password en el archivo passwd (etc/webiopi/passwd) que es asignado en el archivo conf (etc/webiopi/conf) de la librería WebIOPI instalada en el dispositivo. El archivo mencionado contiene el hash del password usado para la autenticación de acceso a la plataforma de control de luces y calefacción.

La herramienta ofrece tres tipos de Crackeo a continuación el resultado para cada método:

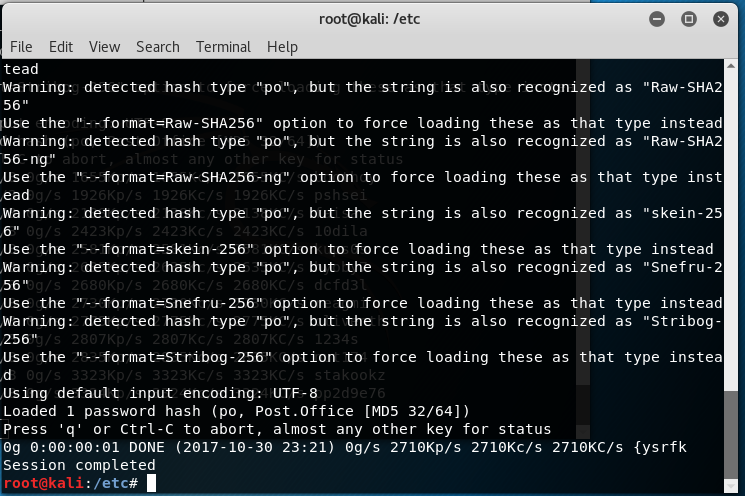
**Single Crack:**

****

**Comando ejecutado: john --single passwd2**

Al realizar la ejecución de este método se puede notar que debido a que es un método que se aplica sobre los patrones “locales” de la maquina donde se está ejecutando el cracking, solo utilizara información tal como la combinación de las letras del usuario del sistema entre otras a fin de aplicar un conjunto de reglas determinado, por tanto este método no permitió crackear el password pero si permitió conocer la cantidad de contraseñas que alberga el archivo.

**Word-List**

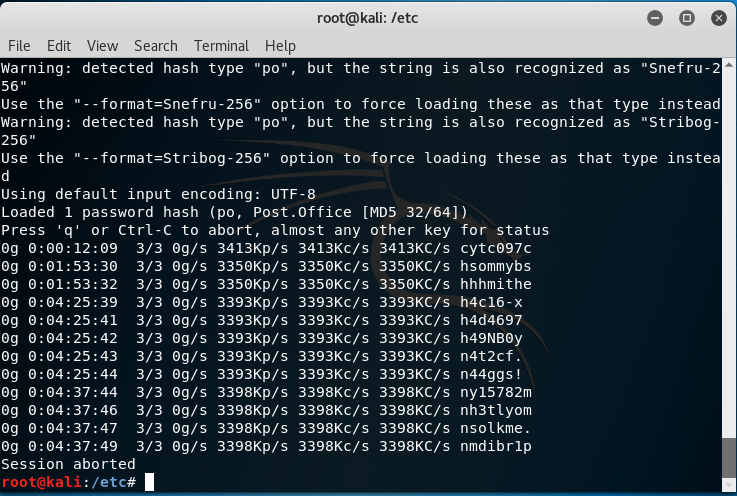
****

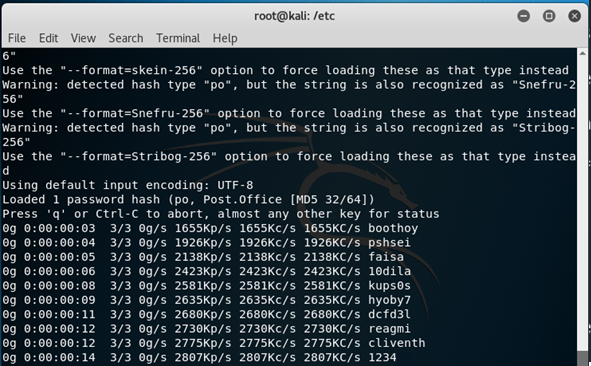
Para ejecutar este método es necesario tener un diccionario de palabras el cual puede ser obtenido desde el siguiente link (<http://download.openwall.net/pub/wordlists/>.) se descarga el archivo all.gz y posteriormente se procede a extraer su contenido. Luego se ejecuta el siguiente comando para ejecutar el crackeo:

**Comando ejecutado: john –wordlist=root/Downloads/all.lst passwd2**

Al terminar obtendremos el password obtenido gracias a l análisis del diccionario el cual puede o no ser el password correcto.

**Brute-force**

****

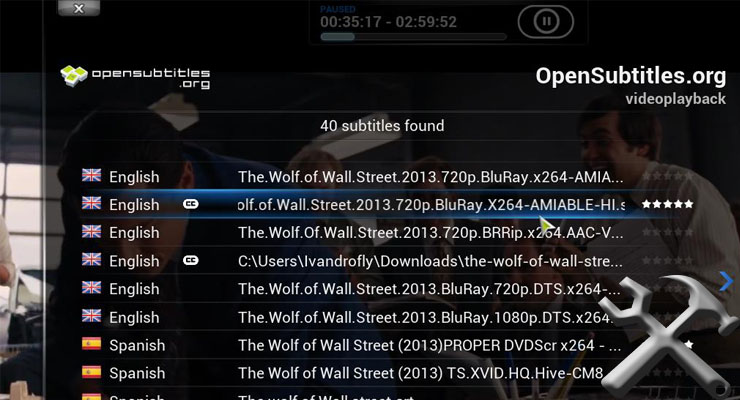
****

**Comando ejecutado: John passwd2**

El método de fuerza bruta el sistema analizara el archivo hasta realizar el crack del password el tiempo dependerá del nivel de seguridad que tenga la contraseña y también de la capacidad de procesamiento de la máquina, para este caso se realizaron dos pruebas con diferentes contraseñas para el primer caso una contraseña alfanumérica (alice34) se realizó la prueba durante 22h y fue imposible determinar la contraseña, después se procedo a cambiar la contraseña por una numérica con una alta tendencia (1234) y el proceso no tardo más de 10 minutos en determinar la contraseña.

**Análisis de seguridad Dispositivo 2 : OSMC (Open Source Media Center)**

Dentro del análisis realizado se instala en el dispositivo addons (aplicaciones) provenientes de fuentes desconocidas y algunas mas de un lista negra de Repositorios infectados (<http://kodi.wiki/view/Official:Forum_rules/Banned_add-ons>). Evidenciando que el dispositivo no tiene control alguno para la instalación de los mismos. Posteriormente se procede a revisar los cambios que presenta el dispositivo después de la infección con el malware.Se percibe que esta vulnerabilidad es de gran impacto en el dispositivo y este depende entonces del contenido del malware.



**Repositorios Instalados en Dispositivo :**

* **OpenSubtitles :** Este addon descarga malware cuando el usuario descarga un archivo de subtítulos.
* **Colossus :** El repositorio a pesar de estar en la BlackList no permite evidenciar afectación alguna en el dispositivo.
* **123Movies :** El addon en si funciona correctamente como un reproductor de peliculas HD, sin embargo hay que tener precaución debido a que el sitio es secuestrado aleatoriamente y cuando esto sucede el atacante empieza a distribuir malware.
* **The Mucky Duck Repo :** El origen del repositorio aparte de venir de una fuente desconocida, concede permisos en la red y en ocasiones puede dejar inutil el uso del servicio de Wifi en el dispositivo.

**Bibliografía :**

* Openwall.com. (2017). John the Ripper password cracker. [online] Available at: http://www.openwall.com/john/ [Accessed 3 Dec. 2017].
* OSMC Forums. (2017). Confusion about OSMC and Kodi, apps, add-ons and programs. [online] Available at: https://discourse.osmc.tv/t/confusion-about-osmc-and-kodi-apps-add-ons-and-programs/19105 [Accessed 3 Dec. 2017].
* OSMC Forums. (2017). Antimalware. [online] Available at: https://discourse.osmc.tv/t/antimalware/15607 [Accessed 3 Dec. 2017].
* Webiopi.trouch.com. (2017). HTTP server. [online] Available at: http://webiopi.trouch.com/CONFIGURATION.html [Accessed 3 Dec. 2017].