KrishnaTeja Veturi

Winter 2016, Project

01/12/2016

**Project: Santoku Linux Wireless Device Forensics**

Device Forensics

* **AFLogical Open Source Edition** – tool used to extract contacts, call logs, messages, and device information. After attaching a device by running this tool it installs a small tool on the target which in return extracts the information sought after. The retrieved information is contained within a .csv file which provides the information in a format accessible by many text viewers.

References:

<https://santoku-linux.com/howto/mobile-forensics/howto-forensically-examine-android-aflogical-santoku/>

<https://www.youtube.com/watch?v=1l6RUjK09bU>

* **Android Brute Force Encryption** – this tool is used to gain the four-digit pin number on a mobile device. The tool extracts header and footer information from the device after it has been rooted. Then the user can do an offline brute force on the encrypted data obtained to pin number to the mobile device. Within Santoku Linus under a virtual machine, approximately 6500 keys can be tested within a minute.

Reference:

<https://santoku-linux.com/howto/mobile-forensics/how-to-brute-force-android-encryption/>

No video for reference however there are steps within the Santoku ‘how-to’ to duplicate.

* **ExifTool** – tool for reading, writing, and manipulating image, audio, and video metadata. Not much info out there but the video shows something pretty cool.

Reference:

<https://en.wikipedia.org/wiki/ExifTool>

<https://www.youtube.com/watch?v=EqcGj9jDNBo>

* **iPhone Backup Analyzer (GUI)** – this tool is used to view backup information created by iTunes for a device that has been stored on a local machine. The tool is capable of retrieving backed up media, such as photos and videos, call logs, messages, GPS information, etc. This tool is also available in other distributions of Linux.

Reference:

<http://tools.kali.org/forensics/iphone-backup-analyzer>

<https://www.youtube.com/watch?v=_nAzyQdaC08>

* **libimobiledevice** - allows other software to easily access the device's filesystem, retrieve information about the device and it's internals, backup/restore the device, manage SpringBoard icons, manage installed applications, retrieve address book/calendars/notes and bookmarks and (using libgpod) synchronize music and video to the device.

Reference:

<http://www.libimobiledevice.org/>

* **scalpel** – (file carving tool) tool that is used to retrieve files that have been deleted from a system. The tool provides the ability to select which particular files are to be un-deleted from the hard drive. Typically, the tool is provided the configuration file containing the information for what files to recover, a director to place the retrieved data, and an image file of the hard disk.

Reference:

<http://www.forensicswiki.org/wiki/Scalpel>

<https://www.youtube.com/watch?v=5Z9JsBazOdw>

* **Sleuth Kit** – This is actually a ‘kit’ of tools that allows the user to analyze a hard disk and retrieve data from it. It is similar to scalpel but provides further tools to retrieve other useful information from a disk.

Reference:

<http://www.sleuthkit.org/index.php>

<https://www.youtube.com/watch?v=VE9mZ4ObVrI>

**Aircrack** – dictionary attack on a packet to retrieve the WPA key for a wireless network. The tool does a brute force attack on the captured packets in order to retrieve the key. However, if the dictionary provided to the tool does not contain the key then it will not be found. In fact, there are huge file dictionaries (>15GB) available online to feed to the tool.

Most videos show how to hack into a WiFi network, however the last step of retrieving the key is using Aircrack.

Reference:

<http://www.aircrack-ng.org/>

<https://www.youtube.com/watch?v=ngxzSlsP1JU>

**Kismet** – a wireless network detector and monitor, packet sniffer, and intrusion detection system that works passively without sending probe packets to networks. It simply listens to the signals that are being broadcasted and logs them to the user’s system to be later analyzed. It is also capable of picking up other wireless sniffers when used as an intrusion system. This tool is also used for wardriving to pick up wireless networks.

Reference:

<https://en.wikipedia.org/wiki/Kismet_(software)>

<https://www.kismetwireless.net/>

<https://www.youtube.com/watch?v=BT8sWlvDJBQ>