Universidad Nacional Autónoma de México

Facultad de Ingeniería

“Introducción a Tails”

Sistemas Operativos

(Reporte de Exposición)

Grupo: 1

Integrantes:

Macario Leonel Falcón

García Hernández Rogelio

08/10/2019

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

A Cypherpunk's Manifesto - Eric Hughes

El Manifiesto Cypherpunk sigue vigente pese a haber sido publicado en 1993. Más que nunca, creo. Porque expresa con claridad abrumadora las prioridades de una sociedad verdaderamente libre, ésa a la cual sirve la criptografía y sus grupos de hackers activistas: los cypherpunks.

Vivimos en una sociedad globalizada, nuestros medios de comunicación prácticamente están automatizados y hemos confiado ciegamente en los fabricantes de las tecnologías que utilizamos. Como sociedad producimos y transportamos información --propia y ajena-- prácticamente todo el tiempo.
Hemos llegado al punto en el que las fronteras entre información personal, privada, secreta quedaron nulificadas a fuerza de una interminable avalancha de servicios, aplicaciones, Internet y sus increíbles redes sociales. Fronteras borradas por nuestra impaciencia, asombro y la nula transparencia de las arquitecturas empleadas por los fabricantes de tecnologías.

En respuesta a esta problemática han surgido proyectos como Tor Projet y Tails, que van muy de la mano.

La red Tor sigue siendo hasta la fecha, una de las maneras más seguras de surfear la web de manera anónima. No se trata de que tengas o no algo que esconder, se trata de preservar nuestra privacidad a toda costa, y dejar de darla por sentada. Todos tenemos información que no queremos compartir con extraños, empresas que husmean todo lo que hacemos solo para bombardearnos de publicidad, y vendernos algo. Redes sociales que te convencen de compartir fotos de tu gato y tus hijos que luego pasan a ser de su propiedad, para venderlas junto al resto de tus datos y hacerse muy ricos.

Tails (*The Amnesic Incognito Live System)* es un tipo de Distribución PELD (*Privacy Enhancing Live Distribution*). Tails es un sistema operativo live que intenta preservar tu privacidad y tu anonimato. Te ayuda a utilizar Internet de forma anónima y evitar la censura en prácticamente cualquier lugar y cualquier ordenador, pero sin dejar rastro a menos que lo pidas explícitamente. Es un sistema operativo completo diseñado para ser usado desde una memoria USB o un DVD independientemente del sistema operativo original del computador. Es software libre y está basado en Debian GNU/Linux.

La distribución en vivo de mejora de la privacidad (o PELD, por sus siglas en inglés) tiene como objetivo proporcionar una solución de software que proporcione al usuario los medios tecnológicos para utilizar tecnologías populares de Internet, manteniendo su privacidad, en particular con respecto al anonimato. Si bien existen diferentes técnicas y servicios que proporcionan esa funcionalidad, esta especificación asumirá el uso de la red de superposición de anonimización de última generación de The Tor Project.

Características de Tails:

- Bloqueo de conexiones automáticas por aplicaciones. Si una aplicación intenta conectarse de forma automática, esa conexión será bloqueada por seguridad.
- Incorpora herramientas criptográficas, como por ejemplo cifrado de dispositivos USB con LUKS (el estándar de Linux para llevar a cabo dicha tarea) o de correos y documentos utilizando OpenPGP.
- Es capaz de correr en una Máquina Virtual.
- Utiliza únicamente la memoria RAM de la computadora anfitriona. De esta forma, hace imposible que mediante un análisis forense del disco rígido de la computadora se pueda llegar a los datos manipulados. De aquí la palabra amnesia.
- Soporta Cold boot attack.
- Permite eliminar archivos de forma segura. Utilizando Nautilus Wipe, verifica que los datos eliminados sean quitados de memoria.
- Prioriza la comunicación HTTPS. Para lograrlo utiliza HTTPS Everywhere, un plugin para el navegador Firefox.

Cold boot attack:

Un **ataque de arranque en frío** consiste en que un atacante con acceso físico a una computadora realiza un volcado de memoria de la memoria de acceso aleatorio de una computadora al realizar un restablecimiento completo de la máquina de destino. Por lo general, los ataques de arranque en frío se utilizan para recuperar claves de cifrado de un sistema operativo en ejecución por motivos de investigación maliciosos o criminales. El ataque se basa en la propiedad de remanencia de datos de DRAM y SRAM para recuperar contenidos de memoria que permanecen legibles en los segundos a minutos posteriores a la desconexión de la alimentación.

Máquinas virtuales:

Una máquina virtual es un software instalado al interior de un sistema operativo que simula en todo y para todo el funcionamiento de una computadora permitiendo la instalación de un segundo sistema operativo perfectamente funcionando

¿Cómo funciona una máquina virtual?
Un programa de máquina virtual es un programa informático que crea un sistema de ordenador virtual, con dispositivos de hardware virtual. Este equipo “máquina virtual” se ejecuta como un proceso en una ventana de su sistema operativo actual. Puede arrancar un

disco de instalación de sistema operativo (o CD en vivo) dentro de la máquina virtual y el sistema operativo será “engañado” creyendo que se está ejecutando en un ordenador real.
El sistema operativo de la máquina virtual se almacena en un disco duro virtual, generalmente un archivo grande, de varios gigabytes, almacenado en su disco duro. Ese archivo es para el sistema operativo como un disco duro real. Esto significa que no tendremos que perder tiempo con la partición.

Las máquinas virtuales añaden algo de sobrecarga, por lo que no será tan rápido como si se hubiera instalado el sistema operativo en hardware real.
Usos de las máquinas virtuales. Las máquinas virtuales nos permiten experimentar con otro sistema operativo sin salir de su sistema operativo actual. Las máquinas virtuales también están aisladas del resto de su sistema, lo que significa que el software en una máquina virtual no puede escapar de la máquina virtual y alterar el resto de su sistema
Por ejemplo si queremos verificar que un programa o una serie de archivos contienen uno o más virus, se pueden probar directamente en la máquina virtual sin que nuestra computadora tenga un problema mínimamente.

Programas para crear máquinas virtuales:

VirtualBox (Windows/Linux/Mac, gratis)
Parallels (Mac)
Vmware VMware (Windows/Linux/Mac)
QEMU (Linux)
Windows Virtual PC (Windows)

¿De que se compone una máquina virtual?

Generalmente, las máquina y recursos virtuales y hardware que administra de la misma forma que administraría un equipo físicos virtuales tienen un sistema operativo. Debe tener un CD/DVD-ROM o imagen ISO que contenga los archivos de instalación de un proveedor de sistemas operativos.

Bibliografía:

- https://es.gizmodo.com/los-cinco-mejores-programas-para-crear-maquinas-virtual-1789667830
- https://azure.microsoft.com/it-it/overview/what-is-a-virtual-machine/
- https://www.fastweb.it/web-e-digital/macchine-virtuali-cosa-sono-e-come-funzionano/
- https://www.eldiario.es/cv/amigoinformatico/Maquinas-virtuales_6_685641440.html
- https://www.activism.net/cypherpunk/manifesto.html
- https://hipertextual.com/archivo/2014/06/que-deberias-usar-tor/