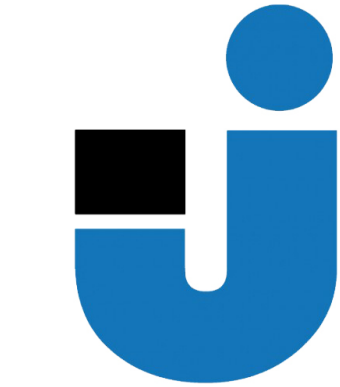


Universidad Nacional
ARTURO JAURETCHE

Seguridad de la Informacióna

TP nº 3: Keyloggers

Salvatori Emiliano

Junio del 2020

Índice

1. Introducción

En el siguiente informe se definen las modificaciones realizadas para la materia **Seguridad de la información Comisión nº 1** para **simular ataques de un ordenador a otro**

2. Objetivos

El objetivo del presente trabajo es el de verificar el funcionamiento de un Keylogger, el cual permite un seguimiento de cada tecla que se pulsa en el host víctima, registrando cada palabra tecleada y casi siempre se hace sin el permiso ni el conocimiento del usuario.

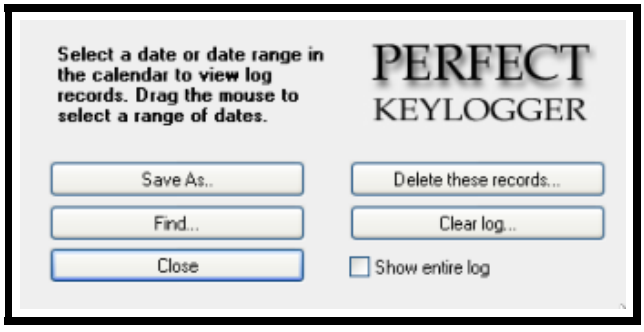
- Generar una máquina virtual con un sistema operativo de tipo **Windows XP**, que actúe como host víctima.
- Conocer las principales vulnerabilidades del Sistema Operativo Windows, ayudándose en este caso con un keylogger denominado **Perfect Keylogger Lite**.
- En base a ello, determinar el comportamiento de un keylogger.

3. Escenario

Se procede a levantar una imagen virtualizada del Sistema Operativo **Windows Xp** con la ayuda del software **VmWare**. Una vez realizado esto, se procede a instalar el keylogger en la máquina huésped.

4. Instalación del Keylogger

Como se puede observar a continuación, el software **Perfect Keylogger Lite** permite el registro de cada uno de lo tipeado en la máquina huésped.

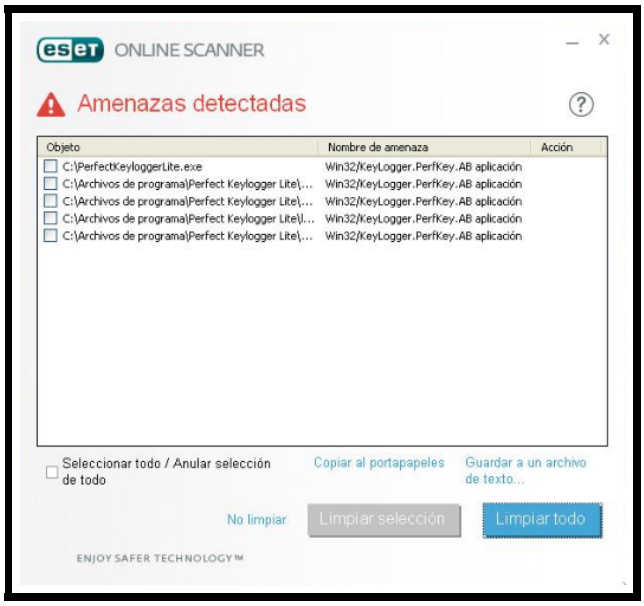


Se puede evidenciar, lo registrado en la víctima.

4.1. Eliminación del Keylogger

Se procede a detectar y eliminar mediante el antivirus **ESET Online Scanner** el programa keylogger.

Se puede visualizar que luego de un escaneo, el keylogger es detectado por el antivirus.



5. Conclusiones

Con este laboratorio, se puede poner el énfasis en lo peligroso que puede resultar no tener medidas de seguridad establecidas y operativas, tanto en empresas como también en particulares. Cabe destacar la importancia de mantener los equipos actualizados, tanto el sistema operativo como las herramientas de seguridad como puede llegar a ser, algún antivirus.

6. Herramientas

6.1. Materiales utilizados para el presente trabajo

Para la resolución del presente Laboratorio se utilizaron las siguientes herramientas:

1. Arch Linux V5.1.11
2. Para la composición del presente Informe se utilizó el paquete *texlive-latexextra 2018.50031-1*
3. Software de Virtualización **VmWare**
4. Software malicioso **Perfect Keylogger**