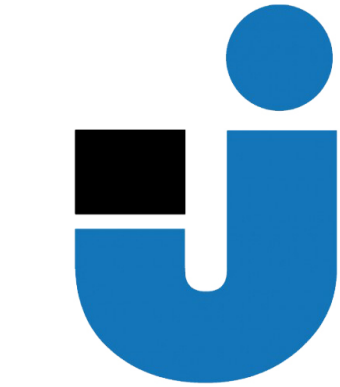


Universidad Nacional
ARTURO JAURETCHE

Seguridad de la Informacióna

TP nº 3: Troyanos

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

La implementación realizada para este trabajo se basa en los siguientes puntos:

- 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 con la aplicación **Optix Pro** creando un troyano para infectar la máquina.
- Para detectar y neutralizar los ataques generados, se utilizan los programas **Local Port Scanner** y **ESET Online Scanner**.
- En base a lo que realizado, poder diagramar un esquema de seguridad para cada host.

3. Escenario

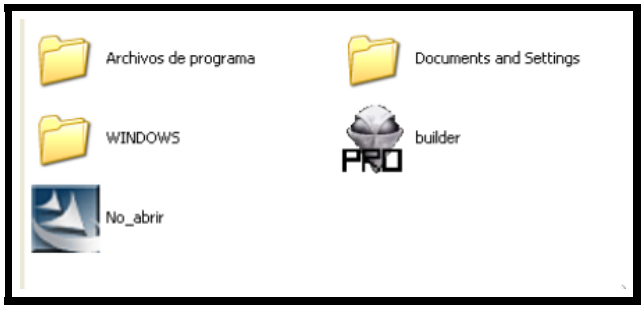
Se procede a levantar una imagen virtualizada del Sistema Operativo **Windows Xp** con la ayuda del software **VmWare**. Una vez realizado esto, se procede a configurar el builder en la víctima para de esta manera, generar el troyano que nos dará acceso a este host.

4. Infección

4.1. Generación del troyano

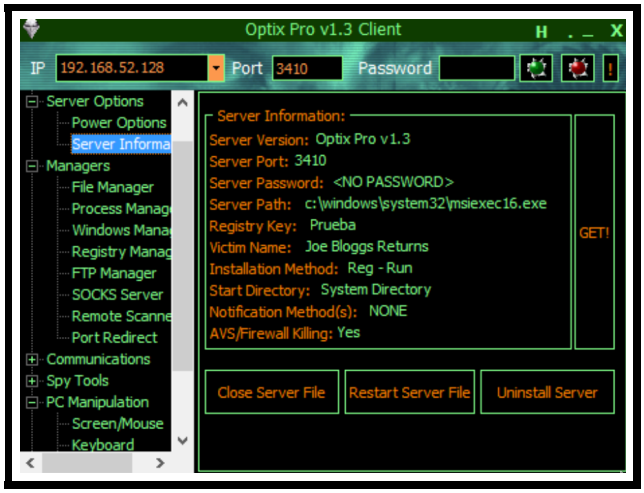
A continuación podemos ver cómo es que el troyano fue configurado de manera exitosa en la víctima y de esta forma podemos proceder a tener control sobre ella.

Ahora bien, una vez que se tiene esta etapa completa, se puede proceder a tomar control del host mediante el programa Optix Pro. La idea es poder colocar el troyano en cualquier parte que sea accesible a la víctima y se inicie automáticamente.



4.2. Toma de Control de la víctima

Una vez ejecutado el troyano, hacemos uso del control de la víctima, por lo que podemos visualizar su información mediante el troyano introducido:



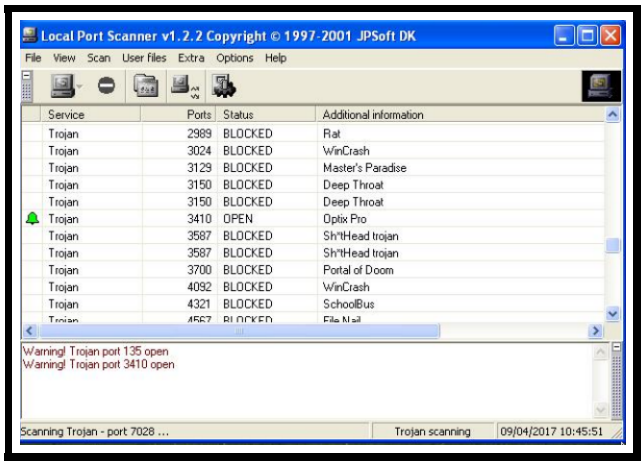
También podemos tomar fotos del host:

5. Desinfección

Como el troyano se introdujo a la víctima mediante puertos abiertos y escuchando a través de la red, procedemos a detectarlo y a eliminarlo. Para el primer paso utilizaremos la aplicación denominada **Local Port Scanner**, para el segundo utilizamos cualquier antivirus actualizado, en este caso haremos uso del llamado **ESET Online Scanner**.

5.1. Bloqueo de puertos

Para clausurar los puertos que se tienen abierto del lado de la víctima, se realiza un escaneo de puertos mediante el mencionado Local Port Scanner.



5.2. Desinfección de troyanos

Como se comentó anteriormente, mediante el escaneo en busca de virus, podemos encontrar la incidencia buscada y a partir de ello poder poner el archivo en cuarentena o directamente eliminarlo.

6. Conclusiones

Como pudimos observar, es de cuantiosa ayuda poder proveer herramientas de protección similares a las utilizadas aquí para que este tipo de archivos no sean transmitidos a los host que estamos tratando de salvaguardar de cualquier ataque malicioso.

7. Herramientas

7.1. 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 **Optix Pro**
5. Software para escucha de puertos **Local Port Scanner**
6. Software antivirus **ESET Online Scanner**