

Prueba Inicial – USB

1. Introducción

Una de las principales fuentes de infección de código malicioso en las organizaciones y los hogares, es a través de dispositivos de almacenamiento externos, tales como USB o memorias infectadas.

Por esta razón, es importante hacer conciencia en los usuarios, de las posibles consecuencias que puede tener el mal uso de los dispositivos tecnológicos, presentes en nuestro día a día y que se conocen muy poco.

La presente prueba tiene como objetivo mostrar al usuario, el hecho de que al encontrarse una memoria USB y acceder al contenido de la misma, puede provocar una infección en su equipo y propagarse por la infraestructura de red de la institución.

Para este fin se tiene un archivo que abre una página en Internet, el cual no es detectado por un antivirus. Éste será guardado en una memoria USB y se dejará “olvidada” en algún lugar concurrido de la institución.

Cuando un usuario encuentre la USB, acceda al contenido de la misma y ejecute el archivo, se abrirá un navegador en su equipo que le llevará directamente a una página Web, en la que se indicarán los peligros que conlleva la acción que acaba de realizar y las medidas de seguridad que deben seguirse para evitar una posible infección en la red institucional.

Es importante indicar que no será identificado ni utilizado ningún dato personal de los participantes en la prueba.



2. Descripción

La presente prueba está basada en un archivo ejecutable dentro de una memoria USB, colocada en un lugar estratégico en calidad de “extraviada”, el cual, al ser ejecutado, muestra al usuario una página web explicando el peligro y las consecuencias de la acción que acaba de realizar. Para ello, deben de seguirse los siguientes pasos:



a. La USB

En primer lugar, será necesario adquirir una memoria USB, la cual podría etiquetarse con el nombre del departamento o área que estará implementando el kit, para hacerla más atractiva y que el usuario en caso de que la devuelva tenga referencia a quién pertenece.

Al guardar el archivo ejecutable en la USB, es recomendable que el archivo vaya acompañado de otro tipo de contenido totalmente inofensivos, por ejemplo, con una carpeta llamada <<Fotos>> y otra <<Trabajo>> donde en cada una de ellas tenga archivos genéricos como imágenes descargadas de Internet, documentos de PDF y/o documentos de Excel o Word. Junto a ellos se ubicará el archivo de prueba, renombrándolo con un título atractivo para cualquier persona como, por ejemplo: “confidencial.exe” o “privado.exe”.

b. El archivo

Se ha realizado un archivo ejecutable, el objetivo de este archivo es abrir el navegador del usuario o, en el caso de que esté abierto, abrir una nueva pestaña, que dirija a la página web de http://anuies-tic.anuies.mx/web/wp-content/uploads/2018/05/Imagen_Prueba_inicial.jpg donde se colocan los peligros a los que se ha expuesto el usuario al haber ejecutado el archivo, así como las medidas que debe de tomar para no provocar una posible infección de código malicioso en la red institucional.

Es fundamental que el archivo sea renombrado con un título<<atractivo para el usuario>>, y si es posible, relacionado con las actividades importantes de la institución.

Este archivo NO es identificado por los antivirus como código malicioso, sin embargo, al tratarse de un archivo ejecutable, es probable que el sistema operativo solicite la confirmación de que se desea ejecutar. Una de los objetivos de ésta prueba, es observar que decide hacer el usuario en este punto.

Una vez finalizada la prueba, se solicitará a los usuarios involucrados, que regresen la USB y eliminen el archivo de su equipo en caso de haber sido copiado.

c. El despliegue

El objetivo de esta prueba es que el usuario encuentre y utilice la USB. Para ello se debe dejar la memoria en ubicaciones públicas estratégicas, en calidad de <<abandonada>>. Algunos de estos lugares pueden ser:





-  Un elevador
-  En la entrada principal
-  Una sala de espera o una cafetería
-  Sanitarios
-  Un pasillo principal
-  Un estacionamiento
-  Un salón de clase
-  Una banca en un área de descanso
-  Una sala de cómputo
-  En la biblioteca
-  Un escritorio

Es importante que la persona encargada de colocar las memorias USB no sea visto durante el proceso.

En caso de que el usuario devuelva la USB al departamento de informática o a cualquier otro responsable, se le explicará la prueba y su finalidad, se le preguntará si revisó el contenido de la misma, o visualizó algún archivo, ya que su equipo posiblemente fue expuesto a un riesgo y se le indicará que hacer en esos casos. Si no la introdujo en algún equipo, felicitarlo por la decisión de devolver la USB sin haberla usado, agradecerle su participación en la prueba y por último se le pedirá no comentar nada al resto del personal y se iniciará de nuevo el proceso, colocando la USB en otra ubicación.

Según el tamaño de la institución y el número de personas, pueden ser colocados varias USB en diferentes ubicaciones, para aumentar la probabilidad de éxito de la prueba.

