TA0004: Privilege Escalation in Adversary Simulation

MONTAJE DEL ENTORNO DE LABORATORIO

JOSU BARRIENTOS (A.K.A. BULW4RK)
BULW4RK@PROTONMAIL.COM
JUNIO DE 2022

Introducción

Con el fin de poder sacar el máximo provecho posible de taller "TA0004: Privilege Escalation in Adversary Simulation" de la V edición del EuskalHack Security Congress, se recomienda cumplir con los siguientes requisitos técnicos para poder participar activamente y poder realizar en vivo los laboratorios del taller. A alto nivel, el taller constara principalmente de lo siguiente:

- Introducción al modelo de seguridad de Windows y a ciertos "Internals" de Windows que afectan de manera directa a los mecanismos de LPE.
- Revisión de múltiples tácticas de LPE y algunos de sus procedimientos, revisando casos prácticos y realizando su identificación y explotación en el laboratorio.

Requisitos Técnicos

Es necesario traer virtualizadas las siguientes máquinas virtuales (se ha comprobado el correcto funcionamiento del laboratorio tanto en VirtualBox y VMware, ambos para Windows y MacOS):

- [**INGLES**] Windows 10 (x64): https://developer.microsoft.com/es-es/microsoft-edge/tools/vms/
    - Instalar la VMware Tools o Guest Additions (Puede ser necesario añadir un Optical Drive para actualizarlos)
    - NOTA: Se deja al asistente traer el Windows 10 que desee, pero necesario que este en idioma global Ingles para evitar colisiones con el script automático de despliegue.
- Kali Linux: https://www.kali.org/get-kali/

Por otro lado, es necesario configurar las redes virtuales del hipervisor de cara a que ambas maquinas se vean entre sí (para poder comunicarse o traspasar ficheros), y que tengan capacidad de conectarse a Internet (es posible que tengamos que descargar algo de GitHub o similar a lo largo del taller). Se pueden dejar sencillamente en modo NAT.

Software Necesario y Preparación de Máquinas

En la máquina Windows 10, es necesario hacer/traer lo siguiente (en orden):

1. Instalar Visual Studio Community 2022 (La máquina de evaluación puede dar aviso de que todas las funcionalidades pueden no funcionar, ni caso y seguir)
    - Instalar entorno "Desktop Development with C++" y ".NET Desktop Development"
2. Descargar Windows Sysinternals: https://download.sysinternals.com/files/SysinternalsSuite.zip
3. Descargar ProcessHacker (Instalar para todos los usuarios durante el Wizard): https://processhacker.sourceforge.io/downloads.php
4. Crear Snapshot de la máquina por si rompemos algo

NOTA: Antes de ejecutar lo siguiente, desactivar temporalmente Windows Defender ya que no le gustan ciertas llamadas dentro de los compilados del script.

5. Script de plataformado automático (Ejecutar como administrador)
    - https://gist.github.com/bulw4rk/4110d8f8a9eae4a0581ca41192554a5e
    - Las tácticas más complejas se introducirán manualmente durante el laboratorio (CredMan, UAC, SocEng, etc.)
6. Descargar repo UACME en c:\euskalhack tras haber ejecutado el PS1
    - https://github.com/hfiref0x/UACME