Principios de Seguridad en Sistemas Operativos
Tarea 1 Evil Maid

Juan José Araya Castro
Alvaro Andrei Miranda Muñoz

August 2022

Código curso: MC1005
Due: Agosto 8, 2022 at 23:59 (CST)
Total puntos: 10 puntos

Introducción

El objetivo del proyecto es lograr el control y manipulación de un computador ejecutando el ataque llamado "EvilMaid". Para lograr dicho ataque se necesita desarrollar una aplicación, código o script que pueda inyectarse en la máquina de la víctima mediante el acceso físico, en donde se conecta un USB booteable que permita la modificación de archivos de booteo del sistema. Para el desarrollo de este proyecto se utilizará el sistema operativo de Linux/Ubuntu.

Instrucciones Generales

Para realizar este ataque es necesario dos maquinas virtuales de Linux para el atacante cualquier versión y el caso del atacado de la versión 18.04 o inferior. Una vez que se configuran los dos equipos por separado el equipo del atacante debe configurar su IP para esperar la respuesta del código inyectado en la PC atacada. Es importante denotar que el equipo atacado debe estar conectado a la misma red del atacante o a internet para poder realizar la conexión del reverse shell.

En la maquina virtual del atacado de debe montar el "USB" del atacante que nuestro caso sera el disco duro virtual, de la maquina virtual configurada como "Atacante". A continuación los pasos para realizar el ataque:

1. Iniciar el sistema de la víctima mediante un usb booteable
2. Montar archivos del sistema de la víctima
3. Obtener permisos de escritura en carpetas de boot

4. Inspeccionar el kernel mediante el binwalk para comprobar los archivos de microcode versus el paquete del initrd
5. Modificar el script con los parámetros que generan el reverse shell
6. Copiar un script dentro de la partición del boot
7. Ejecutar el script para aplicar los cambios y vulnerar la máquina de la víctima
8. Apagar la computadora de la víctima, como si nada hubiese ocurrido, para posteriormente esperar que el usuario siendo atacado encienda la computadora y active el ataque cuando ingrese la clave para desencriptar el sistema operativo

Descripción del Ataque

El ataque de EvilMaid es un caso particular, en donde se requiere acceso físico a la máquina de la víctima. Uno de los ejemplos más icónicos de este ataque se presenta como el de un usario que deja su máquina desatendida en algún sitio, por ejemplo, habitación de un hotel, sala compartida, por que no un espacio de coworking y en el que este usuario deja su máquina desatendida por un tiempo. Este escenario parecería ser parte de una película de ciencia ficción o de acción sin embargo se ha comprobado que en efecto ha sucedido.

Una vez que el usuario ha desatendido su máquina, el atacante reinicia la computadora utilizando un USB booteable. En donde modificando algunos de los archivos de booteo logra remplazar estos archivos con código malicioso que funcionará como la puerta de entrada y la base para un "exploit" del sistema.

Según Wikipedia existen dos tipos de ataques de "EvilMaid":

1. Classic evil maid:
   Ataque en el que se ejecuta ya sea con discos con o sin encriptación y se compromete el firmware de la máquina mediante la modificación de archivos.
2. Network evil maid:
   Ataque en el cual el atacante simula una pantalla de booteo idéntica a la del sistema operativo y envía mediante la red el usuario y el password para accesar la máquina de manera remota.

Por otra parte durante la investigación del proyecto encontramos algunas fuentes que proporcionaban información util para entender las diferentes variantes de los ataques de "Evil Maid".

1. Inyección de Malware:
   Se realiza cuando la máquina carece de clave de ingreso, inyectando con facilidad cualquier código malicioso.

2. Comprometer firmware o BIOS:
   Se roba el user y password de la máquina junto con la información de red, enviándola al atacante.

3. Sidestepping Se esquivan las opciones de seguridad del OS y del boot mediante el DMA (Direct Access Memory) attack

4. Remplazo de panatalla de inicio del Boot:
   Básicamente un ataque de tipo networking de evil maid donde se reemplaza la pantalla de inicio en el booteo de la máquina y este ingresa al sistema operativo de manera transparente mientras envía la información del user y pass al atacante

5. Malas prácticas en el Unified Extensible Firmware Interface (UEFI):
   Para realizar el ataque de EvilMaid de manera práctica y sencilla se debe realizar en sistemas que no implementen las opciones de seguridad del UEFI como por ejemplo, secure boot y el TPM (Trusted Platform Module)

Video ejecución del Ataque

Alvaro Miranda - Juan Jose Araya - EvilMaid Attack v1.0

Autoevaluación

1. Estado Final: Completado
2. Problemas Encontrados: Complejidad de seguridad entre versiones de Linux
3. Limitaciones Adicionales: Estructura y rangos de datos en el tamaño del Kernel (Linux)
4. Reporte de Commits en Git: Commits History
5. Evaluación: 100

Rubro	Puntaje Total	Puntaje Obtenido
Inyección y Ejecución de Evil Maid Attack:	50	50
EM Shell	30	30
Documentación del Ataque	20	20

Lecciones Aprendidas

Este proyecto de Evil Maid nos dejó múltiples enseñanzas que sin duda alguna, nos ha abierto los ojos acerca de lo vulnerables que son los sistemas y las computadoras ante ataques no solo de software, phishing, malware, etc sino de algo tan simple como dejar una máquina desatendida que no tenga o cumpla con los estándares básicos de seguridad. Sin embargo dentro de los puntos más significativos que podemos mencionar se encuentran:

1. En relación a este ataque nos parece que el más importante es, NO dejar la computadora desatendida.
2. En su defecto deshabilitar puertos de USB, CD/DVD
3. Mantener el SO actualizado con las últimas versiones
4. Implementar las recomendaciones, estándares y buenas prácticas de seguridad conocidas en el mercado por los expertos
5. Implementar software de defensa, prevención y detección de ataques

Bibliografía

- Evil Maid: Attack on Computers with Encrypted Disks | SideChannel – Tempest. EvilMaid attack on computers with encrypted disk.
- Pollux's Corner. Implementing EvilMaid attack on Linux with Luks.
- EvilAbigail - Automated Evil Maid Attack For Linux - Darknet. 29 July 2017, EvilAbigail automated evilmaid attack for linux.
- Github: EvilAbigail. AonCyberLabs/EvilAbigail.
- Farooque, Md. Evil Maid Attack. 1 July 2022, Evil maid attack.
- Newest "initrd" Questions. Stack overflow initrd
- Github: EvilMaid attack on encrypted boot. EvilMaid attack on encrypted boot.
- Github: EvilMaid attack on encrypted boot. EvilMaid attack on encrypted boot.
- Github: Topics EvilMaid Topics EvilMaid.
- Github: robertchrk EvilMaid Robertchrk EvilMaid.
- Github: kmille EvilMaid on encrypted boot kmille EvilMaid on Encrypted boot.
- Github: nyxxxie de-LUKS nyxxxie de-LUKS.

- Evil Maid Attack. karpersky evilmaid.
- Evil Maid Attack. 27 Oct. 2021. Wikipedia, Wikipedia EvilMaid attack.