Universidad Internacional San Isidro Labrador

Maestría en Profesional en CiberSeguridad

Curso:

CIB-10 - Seguridad de Sistemas Operativos

Profesor:

Irvin Saenz Cordoba

Tema:

Caso: Evil maid

Estudiantes:

Angélica Ulate Céspedes
Kendal Ureña Rojas

Febrero, 2026

Simulación Evil maid

La estrategia utilizada para este laboratorio fue utilizar un servicio de Linux, ya que una de las grandes limitantes fue poder ejecutar ataques antes del arranque boot. Además, el servicio de Linux favorece en aspectos de configuración y manipulación de comandos.

1. Configuración de acceso TCP

Se creó un puente de conexión entre el atacante y el atacado, por medio de un puerto y una ip local, previamente identificada, que era la dirección ip del atacante. La conexión TCP se abre utilizando el código fuente del archivo adjunto em-shell.py. Como el ejercicio es con fines ilustrativos se decidió crear una lista preconfigurada y segura de posibles comandos a ejecutar por parte del atacante, como evidencia de que la conexión existe.

2. Instalación service de Linux

Desde la máquina atacada se creó un servicio de Linux que contiene un acceso al archivo de ataque .py configurado en otra ruta. Esto asegura que el servicio va a ejecutar antes de iniciar la sesión del usuario, ya que se encuentra localizado en /etc/systemd. El código fuente se encuentra adjunto en el archivo llamado em-shell.service.

3. Conexion del cliente

Se hizo uso de la herramienta nmap, la cual permite crear conexiones con sockets TCP y se usó el siguiente comando para poder abrir la conexión y escuchar la computadora atacada:

```
$ ncat -4 -lvnp 4444
```

4. Autoevaluación

El ejercicio como prueba funciona muy bien mas sin embargo no es un ataque real Evil maid al 100%, mas sin embargo es satisfactorio poder aprender de otras posibilidades para solucinar el problema planeado.

Además, si bien es cierto no hubo que lidiar con problemas de BIOS o secure boot, sí se tuvo que realizar la configuración adecuadamente del servicio que se necesitaba ejecutar desde la máquina atacada.

5. Lecciones aprendidas

Para poder llevar a cabo ataques es recomendado contar con máquinas virtuales, para no afectar el ambiente de la computadora de uso diario.

Se sugiere utilizar Kali linux ya que es muy funcional en temas forenses, de esta forma el usuario se puede familiarizar con el sistema operativo aunque no es completamente requerido, ya que con contar con una distribución debian como por ejemplo Ubuntu también puede funcionar.

Proteger todo lo que se refiere al ámbito personal, en el sentido de utiliza autenticación segura y de 2 pasos, claves fuertes, vigilar los dispositivos físicos, ya que este tipo de ataques específicamente solo puede darse cuando se tiene acceso físico al dispositivo que se quiere hacer el daño.

6. Link del video

A continuación se muestra la evidencia de los pasos realizados como una prueba integrada y funcional:

https://youtu.be/xuqFH5lkAqE

7. Referencias

Nmap Project. (s. f.). Installing Nmap on Mac OS X. https://nmap.org/book/inst-macosx.html

SUSE Documentation. (s. f.). Setting up systemd services. https://documentation.suse.com/smart/systems-management/html/systemd-setting-up-service/index.html

Rutkowska, J. (2009, 23 de octubre). Evil Maid goes after TrueCrypt! The Invisible Things Lab. https://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html

8. Link del repositorio de GIT

Adjunto está todo el código y la version tanto .md como .pdf del documento:

https://github.com/2292an/evil-maid

Asimismo la lista de commits se puede ver desde la siguiente URL:

https://github.com/2292an/evil-maid/commits/main/