XUNTA DE GALICIA

FORMACIÓN PROFESIONAL INNOVA

IES San Clemente

CIFP Rodolfo Ucha Piñeiro

Forense en Linux

1. Consideraciones previas

Las evidencias necesarias se pueden descargar del siguiente enlace:

- mirror1
- mirror2
- mirror3

2. Escenario

Sobre las 17:07 UTC del día 26 de junio salta una alarma en nuestro sistema de monitorización sobre una de las máquinas que tenemos en nuestra red interna. Se cree que podría estar comprometida y que los atacantes habrán conseguido alguna sesión que todavía está abierta. El ataque parece que podría estar realizado desde una máquina de nuestra red interna.

De inmediato se realiza un volcado de la memoria RAM del equipo comprometido y se envía mediante netcat a otra máquina de la red (10.2.0.9). Después se apaga la máquina y se realiza una imagen completa del disco duro en formato EnCase.

Se efectua, además, un interrogatorio entre los usuarios "autorizados" del dicho equipo; y ninguno entre las 16:15 y la hora en que se realizó la adquisición se conectó a el, ni de forma local ni remota.

Se te pide que realices un análisis de evidencias, detectes los vectores de entrada al sistema y las acciones realizadas por los atacantes y generes una línea temporal de las acciones detectadas.

Nota: Para simplificar el análisis podemos descartar cualquier evidencia anterior a las 16:15 UTC.

Evidencias aportadas:

- Captura de memoria RAM.
- Perfil de memoria do equipo para su trabajo con volatility (Ubuntu_3.13.0-24-generic_profile.zip).
- Imagen del disco duro en formato EnCase.

3. Preguntas

1. Cuál es la dirección IP de la máquina víctima? Formato: XX.X.X.X (10 puntos)

   10.2.0.5

2. Cuál es la dirección IP de la máquina atacante? Formato: XX.X.X.X (10 puntos)

   10.2.0.4

3. Sobre qué servicio/protocolo se realizó un ataque de fuerza bruta? Formato: XXX (20 puntos)

   SSH

4. Cuál es el primer usuario empleado en el ataque de fuerza bruta? Formato: XXX (30 puntos)

adm

5. Qué herramienta/comando se empleó para realizar el ataque de Web Fuzzing? Formato (minúsculas): XXXXX (35 puntos)

   wfuzz

6. Cuál es el nombre del proceso sobre el que se ejecuta la shell inversa en la máquina víctima? Formato: XXXXXX.XX (30 puntos)

   server.rb

7. Cuál es el Id del usuario propietario de dicho proceso? Formato: XXXX (30 puntos)

   1124

8. Cuál es el CVE de la vulnerabilidad empleada para el acceso inicial a la máquina? Formato: CVE-XXXX-XXXX (100 puntos)

   CVE-2016-2098

9. Cuál es el nombre del fichero que se compila para hacer la escalada de privilegios? Formato: XXXXXXX.X (50 puntos)

   explotame.c

10. Cuál es el CVE de la vulnerabilidad empleada para la escalada de privilegios? Formato: CVE-XXXX-XXXX (50 puntos)

    CVE-2015-1328

11. Cuál es el nombre de la webshell que dejó activa el atacante en el servidor web? Formato: XXXXX (35 puntos)

    p0wny

12. Cuál fue el usuario de sistema modificado por el atacante para conseguir persistencia en el sistema? Formato: XXXXXXXX (25 puntos)

    www-data

13. A qué hora fue accedido el fichero empleado por la WebShell (Hora UTC)? Formato: HH:MM:SS (75 puntos)

    17:06:58