XUNTA DE GALICIA

FORMACIÓN PROFESIONAL INNOVA

IES San Clemente

CIFP Rodolfo Ucha Piñeiro

Forense en Linux

1. Consideracións previas

As evidencias necesarias pódense descargar da seguinte ligazón:

- mirror1
- mirror2
- mirror3

2. Escenario

Sobre as 17:07 UTC do día 26 de xuño salta unha alarma no noso sistema de monitorización sobre unha das máquinas que temos na nosa rede interna. Crese que podería estar comprometida e que os atacantes terían conseguido algunha sesión que aínda está aberta. O ataque parece que podería estar realizado desde unha máquina da nosa rede interna.

Inmediatamente realízase un envorcado da memoria RAM do equipo comprometido e envíase mediante netcat a outra máquina da rede (10.2.0.9). Despois apágase a máquina e realízase unha imaxe completa do disco duro en formato EnCase.

Efectúase, ademais, un interrogatorio entre os usuarios "autorizados" do devandito equipo e ninguén entre as 16:15 e a hora en que se realizou a adquisición conectouse a el, nin de forma local nin remota.

Pídeseche que realices unha análise de evidencias, detectes os vectores de entrada ao sistema e as accións realizadas polos atacantes e xeres unha liña temporal das accións detectadas.

Nota: Para simplificar á análise podemos descartar calquera evidencia anterior ás 16:15 UTC.

Evidencias aportadas:

- Captura de memoria RAM.
- Perfil de memoria do equipo para o seu traballo con volatility (Ubuntu_3.13.0-24-generic_profile.zip)
- Imaxe do disco duro en formato EnCase.

3. Preguntas

1. Cal é a dirección IP da máquina vítima? Formato: XX.X.X.X (10 puntos)

   10.2.0.5

2. Cal é a dirección IP da máquina atacante? Formato: XX.X.X.X (10 puntos)

   10.2.0.4

3. Sobre qué servizo/protocolo se realizou un ataque de forza bruta? Formato: XXX (20 puntos)

   SSH

4. Cal é o primeiro usuario empregado no ataque de forza bruta? Formato: XXX (30 puntos)

   adm

5. Que ferramenta/comando se empregou para realizar o ataque de Web Fuzzing? Formato (minúsculas): XXXXX (35 puntos)

   wfuzz

6. Cal é o nome do proceso sobre o cal se executa a shell inversa na máquina vítima? Formato: XXXXXX.XX (30 puntos)

   server.rb

7. Cal é o Id do usuario propietario de dito proceso? Formato: XXXX (30 puntos)

   1124

8. Cal é o CVE da vulnerabilidade empregada para o acceso inicial á máquina? Formato: CVE-XXXX-XXXX (100 puntos)

   CVE-2016-2098

9. Cal é o nome do ficheiro que é compilado para facer a escalada de privilexios? Formato: XXXXXXX.X (50 puntos)

   explotame.c

10. Cal é o CVE da vulnerabilidade empregada para a escalada de privilexios? Formato: CVE-XXXX-XXXX (50 puntos)

    CVE-2015-1328

11. Cal é o nome da webshell que deixou activa o atacante no servidor web? Formato: XXXXX (35 puntos)

    p0wny

12. Cal foi o usuario de sistema modificado polo atacante para conseguir persistencia no sistema? Formato: XXXXXXXX (25 puntos)

    www-data

13. A que hora foi accedido o ficheiro empregado pola WebShell (Hora UTC)? Formato: HH:MM:SS (75 puntos)

    17:06:58