HACKTHEBOX

Informe Técnico

Máquina Meow

Este documento ha sido escrito con fines legales y éticos, las técnicas que se explican en dicho documento no se han de realizar con fines maliciosos en situaciones de la vida real.

En este documento se ha utilizado la plataforma **Hack The Box** para simular un entorno controlado para realizar simulaciones de ataques de hacking.

Autor del documento: Miguel Nebot (aka Krathor)

Fecha: 01/06/2024

ÍNDICE:

1. Antecedentes

El presente documento explica el procedimiento a seguir para conseguir comprometer la máquina **Meow** de la plataforma de **Hack The Box.**

Figura 1: IP de la máquina víctima de la plataforma de Hack The Box

Dirección URL

https://app.hackthebox.com/starting-point

2. Objetivos

Estudiar y conocer los sistemas de seguridad de la máquina **Meow**, para poder planificar varias formas de explotación con las cuales poder acceder a la máquina **Meow** y una vez dentro conseguir los máximos privilegios posibles dentro del sistema.

Figura 2: Procesos a seguir para comprometer la máquina **Meow**

3. Análisis de vulnerabilidades

3.1. Reconocimiento inicial

Se inició realizando una prueba de conexión a nivel de red, para asegurarse de que la máquina **Kali Linux** del **atacante** pueda comunicarse con la máquina víctima **Meow**:

```
❯ ping -c 1 10.129.117.253
PING 10.129.117.253 (10.129.117.253) 56(84) bytes of data.
64 bytes from 10.129.117.253: icmp_seq=1 ttl=63 time=36.6 ms

--- 10.129.117.253 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 36.609/36.609/36.609/0.000 ms
```

Figura 3: Prueba de conexión a nivel de red con la máquina víctima

Una vez asegurado que la máquina **Kali Linux** del **atacante** puede comunicarse con la máquina víctima, se utilizó la herramienta **nmap** para realizar un escaneo completo de los puertos de la máquina víctima para comprobar que servicios se ejecutan:

```
❯ nmap -p- -sV --open --min-rate 5000 10.129.117.253
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 19:45 CEST
Nmap scan report for 10.129.117.253
Host is up (0.071s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figura 4: Escaneo de los puertos abiertos de la máquina víctima

Se puede apreciar que hay solo un puerto abierto, el **23** que corresponde al servicio **telnet.**

Telnet es un protocolo a nivel de red que se usa para acceder y administrar dispositivos de forma remota, permitiendo al usuario conectarse a un servidor o dispositivo remotamente y pudiendo controlar dichos dispositivos como si estuviera controlando la máquina de forma directa.

Debido a que este protocolo fue creado en el 1969, carece de las últimas tecnologías de seguridad, ya que la información que viaja a través de este protocolo no está cifrada, permitiendo que un usuario pueda ponerse en escucha por dicho canal de información para conseguir los datos.

4. Acceso a la máquina víctima

En este caso en específico, la máquina atacante puede conectarse directamente con la máquina víctima a través de este comando:

Figura 5: Conexión con la máquina víctima a través del protocolo Telnet

Una vez que la máquina atacante pueda conectarse con la máquina víctima a través de Telnet, hay que iniciar sesión en la máquina víctima.

En este caso, el usuario será 'root':

Figura 6: Conexión con la máquina víctima a través del protocolo Telnet

Esta máquina no requiere de contraseña para iniciar sesión

Al acceder a la máquina directamente como el usuario root, se disponen los máximos privilegios dentro del sistema:

Figura 7: Siendo usuario root con los máximos privilegios

Al listar todos los archivos y directorios dentro del sistema, se puede ver el archivo de la flag de la máquina víctima:

Figura 8: Comando para listar todos los archivos y directorios ocultos del sistema

Figura 9: Archivo flag de la máquina víctima

Para poder ver el contenido de la flag, se puede usar el siguiente comando:

Figura 10: Contenido de la flag

5. Machine pwned

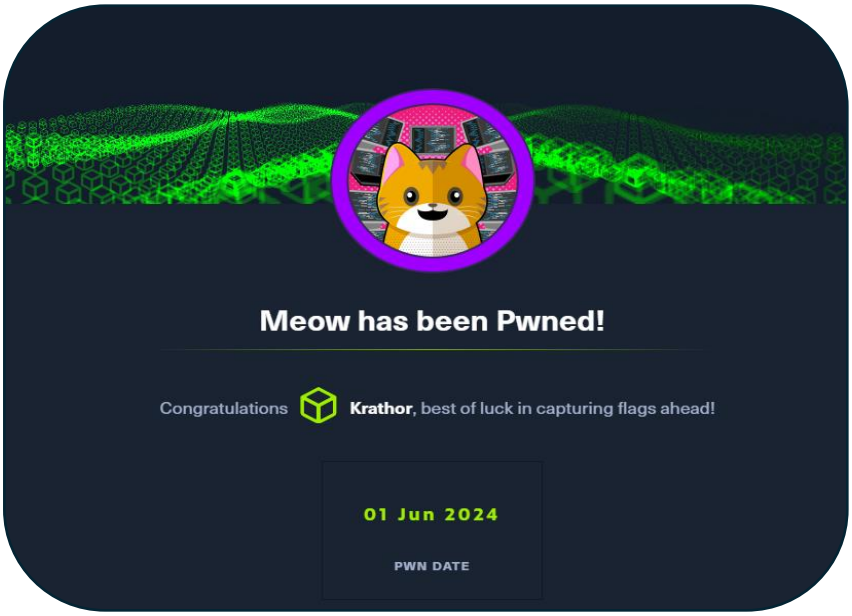

Figura 11: Machine pwned