ESCANER DE VULNERABILIDADES

Existen herramientas de software que exploran todos los servicios de una maquina en busca de versiones de servicios que sean vulnerables de una u otra manera. Vamos a ver una herramienta llamada nikto. Para instalarla como siempre:

```
leurian@asus:~$ sudo apt-get install nikto
```

Para utilizarla es muy simple:

```
leurian@asus:~$ sudo nikto -host 8.8.8.8
```

En lugar de la dirección IP 8.8.8.8 pondremos la dirección del sistema al cual queramos pasarle el escáner de vulnerabilidades (Concretamente este se centra más en vulnerabilidades del servidor web y vulnerabilidades en las páginas web, aunque al igual que nmap será explicado más en detalle en el blog para todos aquellos interesado).

Después habrá que analizar los resultados y ver cuáles son las vulnerabilidades encontradas. Aparecerán en muchos casos códigos de CVE y OVB que son listas de vulnerabilidades que vienen perfectamente documentadas en qué consiste cada una.

CONTRASEÑAS POR DEFECTO

Siempre tendremos la esperanza de que haya una contraseña por defecto en alguna aplicación, lo cual por suerte o desgracia es muy común. Las contraseñas por defecto se refieren a las cuentas que traen los servicios o programas por defecto cuando los instalas. Es decir, que si el administrador no los ha cambiado (en redes grandes es más fácil encontrar algún servicio que haya quedado descuidado con solo mirar las instrucciones de instalación, configuración de la aplicación o servicio) podremos adivinar las cuentas por defecto que usan.