GUÍA TÉCNICA PRÁCTICAS INSTRUCTOR

MÓDULO 4. TALLER 5

TALLER 5: PING SWEEP EN LINUX Y WINDOWS

Realizar un script en lenguaje de programación BATCH o BASH que ejecute un ping sweep en su red LAN en Windows y en Linux.

```
#!/bin/bash
for ip in $(seq 1 254); do
  ping -c 1 192.168.1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d
":" &
done
```

Explicación del código:

Usamos el bucle for do, para el rango 1-254.

Definimos que es lo que queremos ejecutar en el bucle, en este caso el comando ping -c. Ejemplo: ping -c 1 192.168.1.X, ping -c 2 192.168.1.!=X (distinto al anterior). Usamos el $ip para ir "rotando" entre los distintos valores del bucle.

El comando grep para buscar 64 bytes.

Cut -d "" -f 4 para borrar información no deseada.

El comando tr -d para eliminar caracteres repetidos.

Guardar el archivo con el nombre que deseamos, en mi caso pingsweeper.sh.

El siguiente paso es ejecutarlo a través del Shell;

En muchas distribuciones de Linux, incluyendo Kali Linux, el comando ping viene con el bit SUID establecido, lo que significa que se puede ejecutar con los privilegios del propietario del archivo (que es root en este caso). En este caso utlizamos solamente ./pingsweeper.sh