

Guía de ejercicios

- 1.- Realizar un escaneo a un IP de su red y a un IP externo (red pública) usando nmap con la opción Ping Sweep. Interprete los resultados ¿Que diferencia aprecia entre estos dos scanning? Mostrar los resultados y su diferencia.
- 2.- Realizar un escaneo del tipo SYN Stealth al servidor innova.uv.cl, interprete y muestre los resultados. Identifique el sistema operativo.
- 3.- Ejecute el mismo comando anterior pero sumandole la opción -sV, ¿que diferencia puede percibir?, ¿existe algún valor agregado?. Explique
- 4.- Repita el escaneo de la pregunta 3 pero desde la red pública, ¿que diferencia aprecia?, ¿que conclusiones en materia de seguridad puede entregar?
- 5.- Identifique la cantidad y los IP de los servidores FTP, SSH, TELNET, SMTP, HTTP, en la red de a la que pertenece el servidor www.empresa.es.
- 6.- Lanzar una búsqueda de equipos y un sondeo a los host 1 hasta el 90 de la red clase A 10.50.200.0. Debe verificar si los sistemas están ejecutando sshd, DNS, pop3d, imapd o tienen un servidor en el puerto 4564. Para cualquier puerto que se encuentre abierto, se realizará una detección de versión para determinar qué aplicación se está ejecutando.