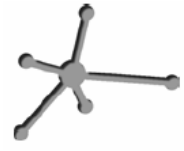




**Universidad Pública
de Navarra**

**Grupo de Redes, Sistemas y
Servicios Telemáticos**



SEGURIDAD EN SISTEMAS INFORMÁTICOS

Cuestiones Práctica 1 Técnicas de Intrusión: los “preliminares”

Guía de Resolución:

II. Pregunta. Se ha de escribir la respuesta correspondiente en la memoria. La memoria se ha de enviar por e-mail a la dirección practicasssi@gmail.com, en formato PDF. En el Asunto (Subject) del correo debe poner “Practica N – Grupo ssiXY” y el nombre del archivo ha de ser de la forma “pracNssiXY.pdf”. N y XY son, lógicamente, los números de práctica y grupo respectivamente

Checkpoint. Se han de mostrar al profesor los resultados obtenidos. No es necesario incluirlos en la memoria. Asegúrese de que el profesor anota que su grupo ha mostrado el Checkpoint.

Bases de datos DNS

II. Explique la salida obtenida por pantalla al teclear el comando `host -a www.telefonica.com`.

Empleando tan sólo el comando `host` encuentre, al menos, 3 IPs de Google que pueda suponer que pertenecen a redes distintas. Muestre al profesor el comando (o secuencia de comandos) que ha ejecutado y la salida del mismo.

II. ¿En qué IP se encuentra el servidor DNS local? ¿Cómo lo ha averiguado?

Bases de datos whois

II. Suponga que es el responsable de seguridad de una red y que detecta un posible ataque procedente de la dirección 130.206.1.1. ¿A qué dirección de correo electrónico enviaría un mensaje denunciándolo? ¿Y si en vez de un ataque hubiese recibido correo basura (*spam*)?

II. Indique el rango de direcciones IP asignado a los servidores de Google Italia.

II. ¿Qué ocurre cuando desde Windows intentamos con `nslookup` forzar que el servidor de búsqueda sea `whois.arin.net`? ¿Por qué?

Herramientas traceroute

II. Localice, al menos, tres puntos de entrada diferentes a la red de `arsys`.

II. ¿Dónde cree que pueden estar físicamente localizados estos puntos de entrada?

II. Compruebe si con `tracert` (Windows) obtiene los mismos resultados que con `traceroute` (Linux). Explique las diferencias, si existen.

II. Si nuestra distribución Linux favorita no incluyese el comando `traceroute`, ¿cómo podríamos implementar de manera rápida y sencilla una herramienta que realizase la misma función? (Pista: revisar el *man* de `ping`)