Test de Intrusión: Reconocimiento y Enumeración

1. Footprinting: Se obtiene una “instantanea” de los elementos observables en la red local (IP activas, protocolos usados, topología, si hay IDS/IPS…)
2. Fingerprinting: Una vez identificadas las máquinas en la red, se escanean para obtener información de estas (Sistema operativo y su versión, servicios activos y sus versiones, Info del IDS o firewall desplegado)

Reconocimiento

- Activo: Interacción directa con el objetivo, se tiene interacción directa con la organización victima. Hay un alto riesgo de detección, se usan barridos de ping o conexiones de puertos de alguna aplicación.
- Pasivo: No se tiene interacción con el objetivo. Se obtiene mediante google, IP o puertos abiertos. Se usa Sniffing.

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=master_cs:int:tm2v2&rev=1779096628

Last update: **2026/05/18 09:30**