1.  
Além do PortScan, algumas ferramentas muito úteis são Shodan (busca na Internet por câmeras e dispositivos expostos), theHarvester (reúne e-mails e subdomínios de fontes públicas), Amass (acha subdomínios usando DNS e bases como CRT.sh), DNSRecon (testa transferências de zona e enumera registros DNS) e wafw00f (detecta firewalls de aplicação web). Cada uma ajuda a descobrir informações que o portscan sozinho não encontra, seja serviços esquecidos, nomes de host internos ou a presença de proteção extra.

2.

No TCP Connect Scan o Nmap faz o handshake completo (SYN→SYN-ACK→ACK) para cada porta, sem precisar de privilégios elevados, mas deixando registro nos logs do alvo. Já o SYN Scan envia só o SYN e, ao receber SYN-ACK, aborta com RST (half-open), exigindo root/administrador e deixando menos vestígios.

3.

Para escapar de um IPS você pode diminuir a velocidade do scan (usar --scan-delay), fragmentar pacotes (-f), usar IPs de distração (decoys com -D), randomizar a ordem de portas e destinos, fazer idle scan (scan via “zumbi”) e até passar por VPNs ou proxies. Essas técnicas tornam mais difícil o IPS identificar e correlacionar o seu tráfego de reconhecimento.