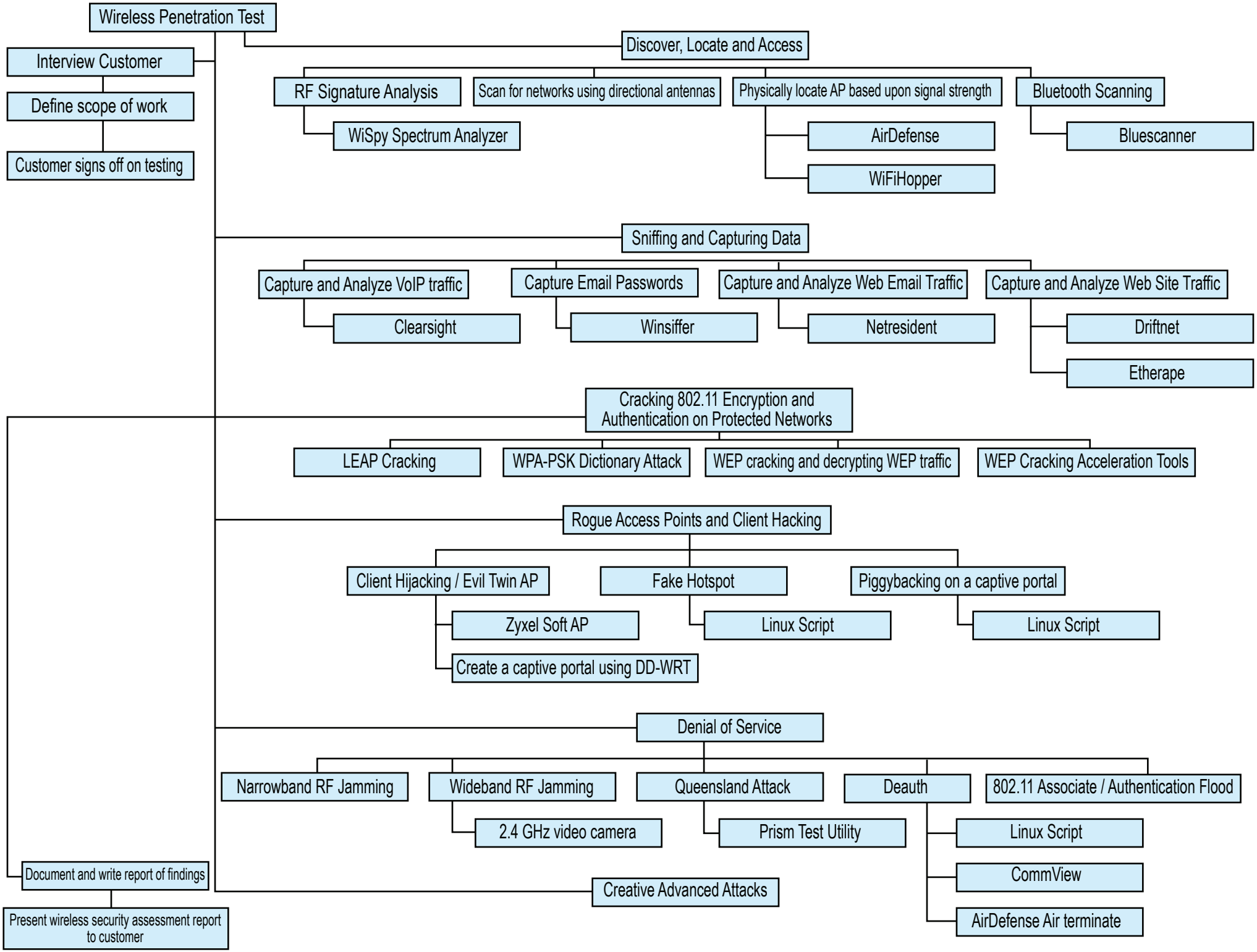
Wireless Penetration Test
Interview Customer
Define scope of work
Customer signs off on testing
Discover, Locate and Access
RF Signature Analysis
WiSpy Spectrum Analyzer
Scan for networks using directional antennas
Physically locate AP based upon signal strength
AirDefense
WiFiHopper
Bluetooth Scanning
Bluescanner
Sniffing and Capturing Data
Capture and Analyze VoIP traffic
Clearsight
Capture Email Passwords
Winsiffer
Capture and Analyze Web Email Traffic
Netresident
Capture and Analyze Web Site Traffic
Driftnet
Etherape
Cracking 802.11 Encryption and Authentication on Protected Networks
LEAP Cracking
WPA-PSK Dictionary Attack
WEP cracking and decrypting WEP traffic
WEP Cracking Acceleration Tools
Rogue Access Points and Client Hacking
Client Hijacking / Evil Twin AP
Zyxel Soft AP
Create a captive portal using DD-WRT
Fake Hotspot
Linux Script
Piggybacking on a captive portal
Linux Script
Denial of Service
Narrowband RF Jamming
Wideband RF Jamming
2.4 GHz video camera
Queensland Attack
Prism Test Utility
Deauth
Linux Script
CommView
AirDefense Air terminate
802.11 Associate / Authentication Flood
Creative Advanced Attacks
Document and write report of findings
Present wireless security assessment report to customer