* Reconnaissance
* Enumeration
* Vulnerability scanning
* Credential attacks
* Persistence
* Configuration compliance
* Evasion
* Decompilation
* Forensics
* Debugging
* Software assurance (including fuzzing, static application security testing [SAST], and dynamic application security testing [DAST])

**10.2.5 Common Tools for Vulnerability Scanning**

There are numerous vulnerability scanning tools, including open-source and commercial vulnerability scanners, as well as cloud-based services and tools. The following are some of the most popular vulnerability scanners:

* OpenVAS
* Nessus
* Nexpose
* Qualys
* SQLmap
* Nikto
* OWASP Zed Attack Proxy (ZAP)
* w3af
* DirBuster
* Brakeman
* Open Security Content Automation Protocol (SCAP) scanners
* Wapiti
* Scout Suite
* WPScan (Wordpress scanner)