OWASP top 10 Methodology listed by top 10 most common vulnerabilities.

1. **Insecure Web Interface.**
   1. Checking for default credentials
   2. Cross site scripting
   3. Sql injection
   4. Cross site request forgery
2. **Insufficient authentication or authorisation.**
   1. Cracking weak passwords
   2. Test the usage of weak passwords
   3. Use proxy sniffers to look for clear passwords or weakly encoded e.g. base64
3. **Insecure network services.**
   1. telnet (hard coded logins)
   2. ftp
   3. finger
   4. tftp
   5. smb
   6. any other open ports?
4. **Transport Encryption**
   1. Bluetooth?
   2. Check for transport encryption
5. **Privacy concerns**
   1. Data collected? Protected?
6. **Insecure cloud and mobile interfaces**
   1. Account enumeration and analysis
   2. Exposed credentials?
7. **Insufficient security configurability**
   1. Granular permissions?
   2. Configuration settings
   3. Security monitoring?
   4. Logging information.
8. **Insecure software /firmware**
   1. File encryption levels
   2. Any sensitive information?
9. **Poor physical security**
   1. Accessible ports
   2. Hardware hacking?

Tools:

* Port Scanner – NMAP
* OWASP Zed attack proxy – used to automatically find security vulnerabilities in web applications
* Nessus / openvas
* Wireshark
* Cain
* Metasploit
* Shodan IOT search engine
* Kali – Bluetooth sniffing. (btscanner – has GUI)(spooftooph)