### Nessus

Nessus is the world’s most well-known vulnerability scanner, which was designed by tenable network security. It is free and is chiefly recommended for non-enterprise usage. This network-vulnerability scanner efficiently finds critical bugs on any given system.  
   
Nessus can detect the following vulnerabilities:

* Unpatched services and misconfiguration
* [Weak passwords](https://www.simplilearn.com/lessons-for-security-professionals-from-worst-passwords-2015-article" \o "Weak passwords" \t "/home/Zeka/Documents\\x/_blank) – default and common
* Various system vulnerabilities

### Nikto

Nikto is a web scanner that scans and tests several web servers for identifying software that is outdated, dangerous CGIs or files, and other problems. It is capable of performing server-specific as well as generic checks and prints by capturing the received cookies. It is a free, open-source tool, which checks version-specific problems across 270 servers and identifies default programs and files.  
   
Here are some of the chief features of Nikto hacking software:

* Open-source tool
* Checks web servers and identifies over 6400 CGIs or files that are potentially dangerous
* Checks servers for outdated versions as well as version-specific problems
* Checks plug-inns and misconfigured files
* Identifies insecure programs and files

### Kismet

This is the best ethical hacking tool used for testing wireless networks and hacking of wireless LAN or wardriving. It passively identifies networks and collects packets and detects non-beaconing and hidden networks with the help of data traffic.  
   
Kismet is basically a sniffer and wireless-network detector that works with other wireless cards and supports raw-monitoring mode.  
   
Basic features of Kismet hacking software include the following:

* Runs on Linux OS, which may be Ubuntu, backtrack, or more
* Applicable to windows at times