**Active Recon – Vulnerability Scanners**

**Scans a host or network for common issues**

* Used to provide a quick way to gather a lot of useful info for an attack
* However, using **just** a vuln scanner is a good way to miss half of the info you’re looking for
* **Nessus**

What to look for:

* Vuln scanners label their finding by critical, medium, low and informational
  + The main focus is critical and medium
* Don’t ignore low or informational tags as these may provide you subtle bits of information required to make an attack work