Penetration Testing Tools

# Nmap

* Network mapper – for network discovery and security auditing
* Free and open source
* Tasks such as
  + Network inventory
  + Managing service upgrade schedules
  + Monitoring host or service uptime
* Uses raw IP packets to
  + See what hosts are available on the network
  + Services (application name and version) the hosts are offering
  + What OS they are running
  + Type of packet filters/firewalls in use
  + Etc.
* GUI and results viewer – Zenmap
* Flexible data transfer, redirection, and debugging tool – Ncat
* Utility for comparing scan results – Ndiff
* Packet generation and response analysis tool – Nping
* Output list of scanned targets with information about them
  + Including the ‘interesting ports table’
    - Port number
    - Protocol
    - Service name
    - State
      * Open – application on target machine is listening for connections/packets on that port
      * Filtered – firewall, filter, or other network obstacle is blocking the port (can’t tell whether it is open or closed)
      * Closed – no application listening on them (could open at any time)
      * Unfiltered – responsive to Nmap’s probes (can’t tell whether it is open or closed)
    - State combinations when it cannot determine which of the two states describe a port:
      * open | filtered and closed | filtered
    - Software version details when version detection has been requested
    - IP protocol scan (-sO)
      * Information on IP protocols than listening ports
  + Reverse DNS names
  + Operating system guesses
  + Device types
  + MAC addresses