**Active Recon – Banner Grabbing**

Common technique used by network scanners like nmap (-a)

* Makes a socket connection to port and waiting for a data response back
* If it doesn’t get one right away, it then sedns a packet and tries to geuess the service off of the response
  + Using the banner

**What is a banner?**

A persistent visible window on a computer monitor that displays the highest level of data accessible during the current session.

Banner grabbing is a technique used by hackers and security teams to gain information about a computer system on a network and services running on its open ports