

**Armitage**

- Can scan remote hosts, find open ports, lookup known vulnerabilities and try to automatically exploit them.

  - `armitage`->`connect`->Yes, run the server for me now

  - `hosts`->`add hosts`, input the host target ip you would like to scan.

  - Right click on newly added host and click `scan`. Should auto detect os and open ports.

  - `Attacks`->`find attacks` finds the known attacks for those hosts.

  - Right click on host and choose the particular vulnerability you would like to try and exploit or for the lazy, just click `attack`->`hail mary` to try each of the attacks in turn until you get a session.