# amass Scan

## Security questions

- amass intel -- use this command and explain what it does and the results
  This command collect OSINT for investigation, by using the domain, IP-Block, organisation name, ASN . Using the reverse whois, whois queries, ip reverse dns, etc.

- amass enum -- use this command and explain what it does and the results
  This command makes horizontal and vertical dns enumeration. Techniques used:

  - SSL Certificates
  - Whois
  - IP DNS Reverse
  - DNS Brute Force
  - and more

- amass viz -- use this command and explain what it does and the results
  Visualization of the gathered data and showing the relation between domain, ip, ASN and more

- amass track -- use this command and explain what it does and the results
  Shows difference between enumerations stored in the database.

- amass db -- use this command and explain what it does and the results
  The graph database can be manipulated with this command. Import, exports, outputs, and more are possible.

- explain if these technique is more interesting than passive reconnaissance The active method is usefully if the target has no protection system for probe the DNS for some RR's or there is no need to be under the radar.
  Bus these techniques of getting information of the SSL, Reverse Whois, brute force, visualization, ... are really interesting. The command are also really useful to compare different timestamp or to automate the reconnaissance.