Host

Host can be used to convert domain names to IP addresses and vice versa:

host google.com

Zone transfers

DNS servers usually have redundant/secondary servers which must be synced to each other. The replication method is called a zone transfer. DNS servers with zone transfers enabled to the public can reveal servers which would not be found by guessing. Zone transfers are typically disabled for DNS servers, but are still worth checking.

Check for zone transfer capability using host, use this command to retrieve the name server:

host -t ns google.com

Then use the name server as an argument in the next command:

host -t axfr -l google.com ns1.google.com

-t quiry type >>>> CNAME, NS, SOA, TXT, DNSKEY, AXFR

-l lists all hosts in a domain, using AXFR