DNS Poking

Setup
modify /etc/hosts
modify /etc/resolv.conf

Nslookup
> server 10.10.10.100
> 127.0.0.1
> 10.10.10.100
> machinename.htb

Host
host -l machinename.htb 10.10.10.13

Dnsrecon
dnsrecon -d <domain(ip)> -r <range>
dnsrecond -d 10.10.10.100 -r 10.0.0.0/8

Dns zone transfer
dig axfr @10.10.10.29
dig axfr bank.htb @10.10.10.29