**Active Recon – DNS**

Zone transfer

* A copy of everything that son the DNS
* Host, IP etc.
* If a DNS is misconfigured, all of this info can be accessed

Dnsrecon -d redteamnation.com

* Name servers
* Mail servers
* Set records

Dnsenum –enum -w

* + - - enum gives 5 threads
  + -w, whois
* Host addr
* Dns servers
* Zone transfer
* Bind versions (linux dns server)

Host -t a facebook.com

* ‘facebook.com has address 157.340.22.35’

Host -t a dev.facebook.com

* ‘dev.facebook.com is an alias for intern-regional.vvv.facebook.com

Intern-regional.vvv.facebook.com has addr 10.110.158.17

Can be used to discover sub-domains

**Nslookup** 157.240.22.36

* Reverse lookup (IP 🡪 Domain)