- Filename: eccouncil-ceh31250-v11-2-12-1-whois-and-dns-recon.md
- Show Name: CEHv11 (312-50)
- Topic Name: Footprinting and Recon
- Episode Name: WHOIS and DNS

==

WHOIS and DNS

Objectives:

- Attain actionable target information like organization owner, name server details, and contact details
- Collect detailed DNS information about target network environment
- Utilize DNS info to create detailed network map

- How familiar should we be with utilizing WHOIS?
    - Thick Model
        - Contains complete info such as...
            - Administrative
            - Billing
            - Technical Contact
            - Domain info
    - Thin Model
        - Only contains the domain's registrar Whois server
- Can you show us?
    - Whois demo
        - It never hurts to VERIFY your target!
- Let's move on to DNS. What info do we get targeting DNS?
    - IP Addresses
    - Domain Names
    - Mail Server Info
        - Demo
            - `nslookup`
            - `dig`
            - `dnsrecon`
- I've heard Zone Transfers are the ultimate goal for DNS enumeration. Why is that?
    - Meant to transfer all DNS info from Primary server to Secondary
    - Will give you a LOT of info
    - Great for helping attackers map out the target network
        - Spoofing
        - Social Engineering
- How would we perform a Zone Transfer?
    - Demo
        - `dig axfr @nsztm1.digi.ninja zonetransfer.me`

- https://digi.ninja/projects/zonetransferme.php