DNS Zone Transfers

THREAT MANAGEMENT

DNS Zone Transfers

- Design to replicate DNS databases between two DNS servers

- This is a vulnerability if zone transfers are allowed, so most prevent zone transfers to servers that aren't trusted

- You can use dig to perform the transfer:

  # dig axfr @dns-server domain.name

Try Performing a Zone Transfer

- DigiNinja provides a couple DNS servers that ALLOW zone transfers for you to practice this technique

- Open up your Linux terminal and try it against nsztm1.digi.ninja and nsztm2.digi.ninja

DNS Brute Forcing

- Used when you can't perform a DNS zone transfer

- Simply sends manual or scripted DNS queries for each IP of the organization

- Organizations can protect against this by sending responses slowly or with IDS/IPS rules to prevent this