**VPNs and DNS Leaks**

**DNS is responsible for resolving domain names into actual IP addresses to connect to**

* The device usually looks in local cache to see if it already knows the IP
* If it can’t, then it’ll send a DNS request to an external DNS server
  + Can specify which DNS server to use within OS
  + If using DHCP, then DNS is usually assigned by router which will then have its primary and secondary servers appointed by ISP
  + ISPs usually run their own DNS server
  + If not available by ISP server, then the query is forwarded through the hierarchy of DNS servers until it can be resolved

**DNS queries happen over UDP port 53 or TCP port 53**

* Usually in plaintext, unencrypted – able to be seen and logged
* VPNs encrypt these queries through their encryption tunnel to their DNS server to avoid ISPs seeing your queries

**DNS being redirected through transparent proxies by ISPs**

* They intercept all DNS queries over UDP/TCP port 53 and force it through their own proxy to a DNS server of their choice, no matter which server you choose in your OS
* To see if this is happening to you, change your DNS server and then head over to ipleak.net and see if your IPv4 DNS server Ips are the same as the ones you changed it to in the OS
  + Mitigation to this is also to use a VPN

n

**DNS poisoning/spoofing**

* ‘Wonderhowto.com: how to spoof DNS on a LAN to redirect traffic to a fake website’
* Not much you can do to get around spoofing and poisoning
* VPN is a solution again to send DNS queries encrypted to external servers
* To mitigate hackers instead of nation states
  + DNScrypt
  + Simple DNScrypt
  + Won’t stop ISPs seeing your traffic, will only stop DNS spoofing from hackers