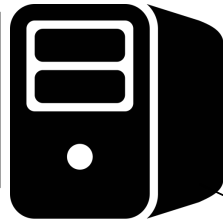


Domain Name System(DNS)

- 13 sets around the world
- Each has unique IP address



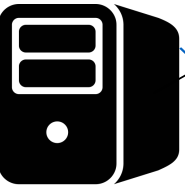
Root Server

TLD: 105.23.65.34



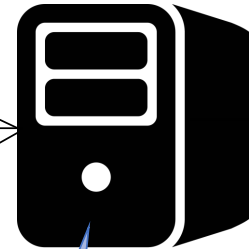
Top Level Domain Server

ANS: 105.23.65.34



Authoritative Name Server

www.wit.ie: 104.20.228.9

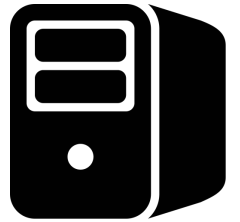


Resolver
(usually ISP assigned)

1. Root, I need IP address for www.wit.ie

3. ANS, I need IP address for www.wit.ie

2. TLD, I need IP address for www.wit.ie



www.wit.ie



www.wit.ie
104.20.228.9



- Address info for top level domains (.com .net .ie .org)

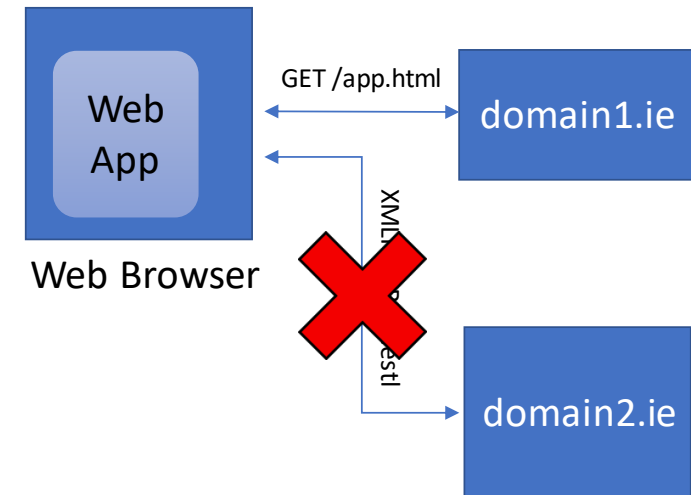
- Responsible for knowing everything about a domain

DNS Rebinding Attack

- Allows remote attack on private network through a victims web browser
- Victims typically initiate attack by clicking on a link or dodgy advert.
- Results in malicious Javascript being downloaded/run in browser
- Browser acts as a “proxy” for attacker to get at victims devices

Same-Origin policy

- Web browsers have built in mechanism called “same-origin policy” that stops web pages making HTTP requests to any domain other than its own.
 - So a page served from one domain (**dodgy.ie**) should not be allowed to contain Javascript that makes requests to other domains (**http://192.168.1.100/set-temperature**)!
- Browsers do this by making sure the protocol, domain, and port of a **URL** is identical to the page requesting it.
 - But do not take into account the IP address.
- **Attackers can get around Same-Origin policy by changing the IP address of http://dodgy.ie in DNS to match http://mybank.ie**
 - Browser would think everything is fine!

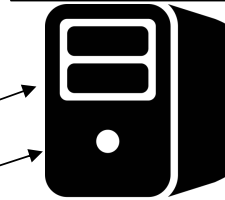


DNS Rebinding – how it works

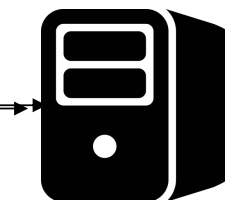


Thermostat Vulnerability

Domain Name	IP
dodgy.net	192.168.1.100
another.net	145.12.45.76
Robber.net	115.66.66.66



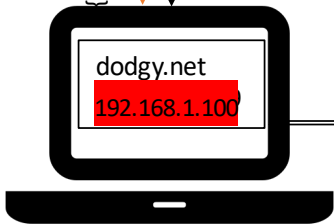
"Bad" Authoritative DNS Server



dodgy.net
144.20.228.9

IoT Device
192.168.1.100

["temperature": 100]



Browser

POST http://dodgy.net/thermo {"temperature": 100}

TTL: 1 sec

Recent publicity Re: DNS Rebinding

- <https://www.wired.com/story/chromecast-roku-sonos-dns-rebinding-vulnerability/>
- https://www.theregister.co.uk/2018/06/21/dns_rebind_attacks_google_roku/
- <https://medium.com/@brannondorsey/attacking-private-networks-from-the-internet-with-dns-rebinding-ea7098a2d325>